

#4

⑩ 日本国特許庁

公開特許公報

発明の名称
アンソルツキ
電子装置

2. 発明者
氏名 アメリカ合衆国ニューヨーク州、一レーヴィー・オーバーリンク・ドライブル
氏名 ワイリアム・ダフ・エイバード(他4名)

3. 特許出願人
住所 アメリカ合衆国10504、ニューヨーク州
アーモンク(省略なし)
名前 インターナショナル・ビジネス・マヘンズ・コーポレーション
(709)
代表者 ジエイ・エイア・グレイデイー
国籍 アメリカ合衆国

4. 代理人
住所 郵便番号 104
東京都渋谷区六本木三丁目2番12号
日本アーヴィング・エム株式会社
TEL(代表)586-1111
氏名 分野士 小野威司
(6454)

5. 送付書類の目録
(1) 明細書 1通
(2) 図面 1通
(3) 特許成狀文 各1通
(4) 优先権成狀文 各1通 51.2.18
(5) 出願審査請求書 1通

明細書

1. 発明の名称 電子装置。

2. 特許請求の範囲

(1) 一組の暗号キー・ピントの列のものとデータ・ピントのブロックに対して横ブロック暗号化操作を実行するための暗号装置にして、上記データ・ピントのブロックを記憶するための記憶手段と、

上記一組の暗号キー・ピントを置換して出力するための第1級形変換手段と、

上記記憶手段に接続され、上記データ・ピントのブロックを記憶することによって、上記第1級形変換手段から出力された暗号キー・ピントの数に等しいデータ・ピントのブロックを生成するための手段と、

該手段からの出力されたデータ・ピントのブロック及び上記第1級形変換手段からの置換された暗号キー・ピントに従つて代替変換を実行することにより、元のデータ・ピントの数に等することにより、元のデータ・ピントの数に等する。

⑪ 特開昭 51-108701

⑫ 公開日 昭51. (1976) 9. 27

⑬ 特願昭 51-16096

⑭ 出願日 昭51. (1976) 2. 18

審査請求 有 (全32頁)

序内整理番号

6964	53
7240	53
7165	56

⑮ 日本分類

9601D0	H04K 1/00
9601A1	H04L 9/00
9701E2	G06F 3/00

しいビット数を有する代替ビット群を生成するための手段と、

該手段から出力された上記代替ビット群を復元することにより、上記データ・ピントのブロックの横ブロック暗号を生成するための第2級形変換手段とを有することを特徴とする暗号装置。

(2) 上記代替ビット群を生成するための手段が、並置されたデータ・ピント及び置換された暗号キー・ピントを組合わせて新しい一組のピントを生成するための手段と、

該手段から出力された上記一組のピントに対して非線形代替変換を施すことにより上記代替ピント群を生成するための非線形置換手段とより成ることを特徴とする特許請求の範囲第1項記載の暗号装置。

Best Available Copy

3発明の詳細を説明

本発明は、データ処理環境のもとで利用される暗号装置に関するものであり、更に具体的には、データの機密保護及びプライバシーを確立するため、デジタル・データを暗号化したり解読したりするのに使用され得る横ソルンク暗号プロセスを実行するための暗号装置に関するものである。

コンピュータ・システム・ネットワークにおける遠隔通信の利用、端末即ち入出力装置と制御装置との間の非常に長いケーブル接続の使用、及び記憶媒体の移動可能性が各々増大するにつれて、データの物理的な保護が一般に保証され得なくなってきたために、データの收受又は譲り受けする擔心が高まってきた。暗号方式は、データの伝送媒体よりもむしろデータ自身を保護するという点において、データの機密性及びプライバシーの保護を達成するための1つの手段として認められている。

これまでにも、データ通信の機密保護及びプライバシーの保持を目的として、メッセージを暗号

化するための種々のシステムが開発されている。そのようなシステムの1つに、プロトクル全体が所定の暗号キーに基づいて代替(=substitution)されるようなクロック暗号システムがある。代替されたメッセージは、暗号キーを知らなければ理解され得ない暗号テキストになる。所定の暗号キーに基づいて処理が行なわれる代替技術(substitution technique)の利点は、この暗号キーを適応することによって解読操作を簡単に実行できることにある。代替技術の設計及び原理に関する更に詳しい説明は、例えば1949年10月に発行されたBell System Technical Journal, 第28巻、第656~715頁に掲載されているC. E. Shannonによる"Communication Theory of Secrecy Systems"と題する論文及び1973年5月に発行されたScientific American, 第228巻、第5号、第15~25頁に記載されているH. Feistelによる"Cryptography and Computer Privacy"と題する論文に見出される。これら

2つの論文には、2以上の暗号が、例えば非線形代替及びこれに続く線形変換といった連続的な段階によって、連続的に組合わされるような複雑な暗号システムについての詳しい説明がなされている。

データ処理システム内のデータの機密保護及びプライバシーを改善するため、種々の暗号システムが開発されてきた。例えば本国特許第3798359号明細書には、非暗号テキスト・メッセージ(暗号化されていないメッセージ)の横形変換及び非横形変換を組合せた横幅1システムが開示されている。これらの变换は、一意的な暗号キーを用いて行なわれ、このキーの関数になつてゐる。暗号キーは、変換を制御することの他に、暗号システム内で種々のレジスタ代替及び部分的に暗号化されたデータのモジュロ2加算の制御も行なう。しかしながら、上記本国特許明細書には、キー経路指定器によるモジュロ2加算器への暗号キー・ビットの正確なマッピングの説明や、代替機能ボックス内で実行される特別の非横形変換又は分散器(difusor)によって実行される暗

別の置換(permutation)の説明しこれらはすべて暗号処理操作の質に重大な影響を及ぼすものである)については、何ら開示されていない。暗号キーは、幾つかの小さなグループに分けられ、各グループに含まれる暗号キー・ビットは、暗号処理操作が隠匿される前にシフトされる。各グループに含まれる暗号キー・ビットの数が比較的小少なため、各暗号キー・ビット・グループの並び順効率は、暗号処理操作の隠された部分に限定される。これもまた、暗号処理操作の質に影響を及ぼすものである。更にこのシステムでは、暗号キー・ビットのみの関数として選択された2種類の代替機能ボックスだけが使用されているが、これも同様に暗号処理操作の質に影響を及ぼすものである。

上記のシステムに關連して、本國特許第3796830号明細書には、非暗号テキストのプロセスがセグメント単位で処理されるような複雑な暗号システムが開示されている。各セグメントは、暗号キーの一節に基づいて、逐次に変換される。しかし

ながら、このシステムはその性質において並列式であるためにスループット速度が遅く、またもしこれを並列式に変更しようとすれば、そのハードウェアはかなり複雑になる。更に、前述のシステムと同様に、このシステムもまた同じような2種類の代替機能がソクスのみに限定される。

本発明に従えば、任意に選ばれた1つの暗号キーの割当のもとに、32ビットのデータ・ブロックを暗号処理(暗号化又は解読)し侍る暗号装置が提供される。この暗号装置は、全記憶52個のデータ・ビントを有し且つ各々が4個のデータ・ビントより成る8個のセグメントに分けられたデータ・ブロックが、6個のデータ・ビントを各々有する8個のセグメントを構成する48個のデータ・ビントのブロックへ並張されるような操作を実行することにより、暗号処理を行なう。このようないくつかデータ・ビントの並張は、8個の4ビット・セグメントの各々のエンド・データ・ビント、例えば最初の2ビットを二重にすることによつて達成される。8個の4ビット・セグメントとみなす

れる並張された48個のデータ・ビントは、任意に決められた順序に従つて選択される。8個の6ビットキー・ビント・セグメントとみなされる。8個の暗号キー・ビントとモノクロ2加算によつて組合せられる。モノクロ2加算の結果の8個の4ビント・セグメントは、8種類の非アフィン変換のための実際の引数を構成する。各置換操作においては、先行の6ビント・セグメントの二重にされたエンド・ビント及び置換された暗号キー・ビントのモノクロ2加算と、後続の6ビント・セグメントの二重にされたエンド・ビント及び別の置換された暗号キー・ビントのモノクロ2加算との結果として生じた6ビント・セグメントの2個のエンド・ビント(両端のビント)が解説されて、各々16個のエントリーを有する4個の機能テーブルのうちの1つが選択される。各エントリーは4ビットから成つている。次に、この6ビット・セグメントの複り4個のビントを解説することにより、選択された機能テーブルの16個の4ビント・エントリーのうちの1つが選択される。各セ

グメントに対する置換操作に対する機能テーブルは互いに異なつており、従つて、8種類の異なる置換操作が行なわれて、32ビットの代替セントを規定する8個の4ビット・セグメントが生じる。なお、本明細書において、「代替」とは取るビント・ブロックが別のビント・ブロックへ代えられることを意味し、「置換」とは取るビント・ブロック内においてビントの順序が変更されることを意味する。次に、この32ビットの代替セントは、任意に決められた置換による幾形置換を受ける。このような非線形置換及び線形置換の組合せにより、32ビットのデータ・ブロックの新ブロック暗号が生成される。

上述の種ブロック暗号処理操作は、暗号脚数及びキー・スケジュール間数によつて規定され得る般ブロック暗号処理アルゴリズムに従つて、16回繰返して実行される暗号化プロセスに使用される。かくして、暗号化プロセスにおいて、もし64ビットの入力メッセージ・ブロックが32ビットの1ブロック及び32ビットの1ブロックから成つていると、この入力メッセージ・ブロックは項Rで表わされる。また、もし暗号キー・ビントのブロックが暗号キーKEYから選ばれるならば、このブロックは項Kで表わされる。従つて、最後のものを除くすべての繰返しがついては、入力が正の時の出力は項L'で表わされる。これは、次のように定義され得る。

レ'の定義

(1)

$$k' = L \oplus i (R, k)$$

上式において、 \oplus はビント毎のモノクロ2加算(拡張的オア)を表わし、各繰返し操作の間に、暗号キーKEYから暗号キー・ビントの異なつたブロックKが選ばれる。最後の繰返しを除く各繰返

特明 昭51-108701(4)

$$L_n = R_{n-1} \quad (4)$$

$$R_n = L_{n-1} \oplus f(R_{n-1}, K_n) \quad (4)$$

最後の繰返し操作の出力は互換されないので、
nが16の時の最後の繰返し操作の出力は次式で
定義され得る。

$$L_n = L_{n-1} \oplus f(R_{n-1}, K_n) \quad (5)$$

$$R_n = R_{n-1}$$

した後に出力が互換(transpose)されるので、
入力がL'の最後の繰返しにおける出力は、次式
で定義され得る項L'R'で表わされる。

$$\begin{aligned} L' &= L \oplus f(R, K) \\ R' &= R \end{aligned} \quad (2)$$

更に、もしキー・スクエニールKSが1から1
6までの範囲にある整数n及び暗号キーKEYから
の関数として定義されるならば、暗号キーKEYから
の暗号キー・ビットの互換された値は、次式
で定義される項K'nによつて表わすことができる。

$$K_n = KS(n, KEY) \quad (3)$$

かくして、L'及びR'が各々L及びRであり且つL'及びR'が各々L'及びR'であれば、
nが1から15までの範囲にある場合の繰返し操
作の出力は次式で定義され得る。

暗号化プロセスにおいては、K1が最初の繰返
しで使用され、K2が2回目の繰返しで使用され、
以下同様にして、最後の16回目の繰返しでは
K16が使用される。本発明に従う暗号化アルゴリズムを用いることの暗号化ブ
ロセスの一例が図8に示されている。

暗号関数f(R, K)は、選択関数と呼ばれる
原始関数及び置換関数によつて定義され得る。か
くして、もし32ビットのブロックRが48ビット
のブロックへ拡張されるならば、拡張されたブ
ロックは項E(R)で表わされる。この拡張され
たブロックE(R)は、任意に決められた直線に

並つて選択された暗号キー・ビットのブロックR
とモジュロ2加算で組合わされ、8個の4ビット
・セグメントB1, B2, ..., B8が生成される。
これらのセグメントは、8種類の異なる選択関
数S1, S2, ..., S8に対する引数を構成する。
並つて、モジュロ2加算は次のように定義され得
る。

$$E \oplus K = B_1, B_2, B_3, B_4, B_5, B_6,$$

$$B_7 \text{ 及び } B_8 \quad (6)$$

各選択関数S1, S2, ..., S8は、4ビット・セグメントB1を
4ビット・セグメントへ変換し、このため8個の
異をつた選択関数はS1(B1), S2(B2), S3(B
3), S4(B4), S5(B5), S6(B6), S7(B7)
及びS8(B8)として定義され得る。次に、8
個の選択関数の8個の4ビット・セグメント巾刀
は、32ビットの单一ブロックへ組合される。こ
の32ビット・ブロックは、置換関数Pによつて、
次のように表わされる新しい32ビットのブロ
ックへ交換される。

$$P(S1(B1), S2(B2), \dots, S8(B8)) \quad (7)$$

これが暗号関数f(R, K)を表わす。

本発明に従う暗号プロセスは、前と
同じようく暗号関数及びキー・スクエニール関数
によつて規定され得る種ブロック暗号処理アルゴ
リズムによつて、16回繰返して実行される解読
プロセスにも使用され得る。かくして、もし暗号
され元の4ビットの入力メッセージ・ブロック
が、32ビットの1ブロックL'及び32ビット
の1ブロックR'から成つていると、この暗号化
された入力メッセージ・ブロックは項L' R'で
表わされる。従つて、入力がL' R'の最初の繰
返しにおける出力は、互換された形で現し且て表
わされ得る。これは、次のように定義することができる。

$$\begin{aligned} L &= L' \oplus f(K, K) \\ R &= R' \end{aligned} \quad (8)$$

この場合、各繰返し毎に暗号キーKEYから出
られる暗号キー・ビットの異なるブロックRは
暗号化操作の時に選ばれた順序とは反対の順序で

特開昭51-108701(5)

解説操作においては、最初の繰返しに K_{11} が使用され、2回目の繰返しに K_{12} が使用され、以降同様にして、10回目の繰返しでは K_{10} が使用される。本発明に従う積ブロック暗号処理アルゴリズムを用いることによる解説プロセスの例が第8図に示されている。

従つて本発明の目的は、暗号キーの割当のもとにデータ・ブロックを暗号処理するための暗号装置を提供するにある。

本発明の他の目的は、暗号キーの割当のもとにデータ・ブロックを暗号処理するための取扱プロセスを提供するにある。

本発明の他の目的は、暗号キー及びデータ・ブロックに従つて割当される非線形変換を含む積ブロック暗号処理プロセスを提供するにある。

本発明の他の目的は、多収対1の非線形変換を含む積ブロック暗号処理プロセスを提供するにある。

本発明の他の目的は、暗号処理されるべきデータ・ビットのブロックが、これらのデータ・ビン

選ばれる。最初の繰返し後は、後続の各繰返しは最後のものを除いて互換され、従つて入力がしり R' の後続の各繰返しにおける出力は、次の式で定義される項 L'_R によって表わすことができる。

$$L = R' \oplus f(L', K) \quad (9)$$
$$R \sim L'$$

かくして、もし L_n 及び R_n が各々 L 及び R であり且つ L_n 及び R_n が各々 L' 及び R' であれば、 n が 15 に等しい時の最初の繰返しの出力は次のように表わすことができる。

$$L_{n-1} = L_n \oplus f(R_n, K_n) \quad (10)$$
$$R_{n-1} = R_n$$

最後の繰返しを除く各繰返し後に出力が互換されるので、 n が 15 から 1 までの範囲にある場合の後続の各繰返しの出力は次式で定義され得る。

$$L_{n-1} = R_n \oplus f(L_n, K_n) \quad (11)$$
$$R_{n-1} = L_n$$

トのうちの所定のものを二重にすることによつて拡張されるような、また一組の暗号キー・ビント並びに一組のデータ・ビント及び二重にされたデータ・ビントに従つて割当される非線形変換部を含むような積ブロック暗号処理プロセスを提供するにある。

本発明の他の目的は、暗号処理されるべきデータ・ビントの一群の並列セグメントが、各セグメント中のデータ・ビントの所定のものを二重にすることによつて拡張されるような、また一組の暗号キー・ビントを含む一群の並列セグメント並びにデータ・ビント及び二重にされたデータ・ビントを含む一群の並列セグメントに従つて割当される一群の非線形変換機能を含むよりな積ブロック暗号処理プロセスを提供するにある。

前にも触れたように、データ処理ソフトワークの内部においては、データの傍受又は更替や、記憶媒体の物理的取外しに対して、ネットワークを物理的に保護することは極めて困難である。この問題は、データが通信機を介して通路保全と遅延削除ユニット又は遠隔端末との間でやりとりされる場合、非常に長いケーブル接続を介して削除ユニットと接続即ち出入力装置との間でやりとりされる場合、又は移動可能な記憶媒体が設置されている場合において最も顕著に生じる。このような状況のもとでデータの機密保護を達成し、プライバシーを守るために1つの手段として、ネットワーク内の重要な場所に暗号装置が設置される。送信局においては、暗号化モードで動作する暗号装置によつて非暗号データが暗号化された後、この被暗号化データが受信局の万へ伝送される。受信局側では、解読モードで動作する暗号装置を用いて、伝送された被暗号化データを解読することにより、元の非暗号データが得られる。受信局及び送信局の役割が反対になつた時、即ち今まで

受信局として働いていたところが送信局になり且つ送信局として働いていたところが受信局になつた時には、各々の局に設置されている暗号装置も同様に今までとは反対のモードで動作される。第1図は、代表的なデータ処理ネットワークにおける暗号装置の設置場所を例示したものである。第1図の例では、暗号装置は無い丸印の部分に設置されている。

第2図は、8ペイトからなる64ビットのデータ・ワードDW即ちデータ・メッセージ・ブロックを暗号化又は解読するための暗号装置を示したものである。図において、太い実線の途中にある丸印で囲まれた数字は、各々の母線を介して送られるビットの数を表わしている。各ペイトは8個のデータ・ビットを含んでいる。メッセージ・ブロックのデータ・ペイトは、データ・バス・インを介して一時に1つずつ逐次に暗号装置へ印加され、併せて、64ビットのメッセージ・ブロックを完全に転送するには、8サイクルを必要とする。暗号装置に受信された各ペイトは、通常の交換配

列PICKS 50(以下、PICKSといふ)によつて実行される初期整形演算(ピント順序の変換)を受ける。次いで、各々の置換されたデータペイトは2つに分割されて、奇数番目のピント0、2、4及び6が上部入力バス(以下、UIBと略す)100に印加され、奇数番目のピント1、3、5及び7が下部入力バス(以下、LIBと略す)150に印加される。UIB:100及びLIB:150は、直列-並列変換を行つて、併せて、メッセージ・ブロックの8ペイトが受信された後、UIB:100はメッセージ・ブロックの第1半分の32ビットを上部データ・レジスタ(LDR)200へ並列に供給し、一方LIB:150はメッセージ・ブロックの残り32ビットを下部データ・レジスタ(LDR)250へ供給する。

64ビットのメッセージ・ブロックが受信されると、UIB:100及びLIB:150へバス(以下、各々が7個のキー・ビット及び1個のパリティ・ビットを含む8個のキー・ペイトを供給する64ビットの外部レジスタから暗号キ

ーが入力される。この暗号キーの各暗号キー・ペイトは、8番目のビット即ちパリティ・ビットを除いて、一時に7ビット・ペイトずつキー・バス・インを介して暗号装置へ印加される。この場合も、暗号キーを完全に転送するには、8サイクルを必要とする。上述のノッセージ・ブロックと同様に、暗号装置に受取られた各暗号キー・ペイトもPICKS 50による初期整形を受け、この後、暗号キーの各々の置換されたペイトは2つに分割されて、各7ビット・ペイトの最初の4ビットが上部キー・レジスタ(UKR)350へ印加され、残りの3ビットが下部キー・レジスタ(LKR)400へ印加される。UKR350及びLKR400は各々28個の段を有し、UKR350の最後の段が LKR400の25番目の段に接続されている。UKR350及びLKR400は共に直列-並列変換を行ない、8個の7ビット・ペイト(各々が8ビットを含む7個のグループと考えられる)が逐次に受取られている間に、これら7グループのうちUKR350の段0、8及び

16へ各々逐次に受取られた8ビットよりなる3グループと、LKR400の段0、8及び16へ各々逐次に受取られた8ビットよりなる3グループとが、各々3個の並列8ビット・グループへ接続される。これら2つの3グループは、UKR350及びLKR400における24ビットの2つの並列グループとみなされる。7個の8ビット・グループの残りのダブループは、UKR350の段24へ逐次に受取られる。UKR350の最後の段 LKR400の段24とが接続されているので、UKR350へ逐次に受取られた残りの8ビット・グループの最初の4ビットは、LKR400へ送られて、その残りの4段において4ビットの並列部分グループへ接続され、次の4ビットは UKR350の残りの4段において4ビットの並列部分グループへ接続される。かくして、UKR350及びLKR400は、各々が28ビットの2個の並列グループとみなされる暗号キーを含む。この時点においては、ノッセージ・ブロックの第1半分及び第2半分が各々UIR200及びL

DR250へ転送され、そしてUKR350及びLKR400には符号マーがロードされているが、一旦UKR350及びLKR400へロードされると、これら2つのレジスタ間の操作はこれ以上使用されず。UKR350及びLKR400は、各々28ビットの独立したシフト・レジスタとして動作する。符号化プロセスにおいては、UKR350及びLKR400の符号マー内容が1ビット位置を往復するシフトされた後、16位のみ調し操作が並列的に行われる。符号化プロセスの繰り返し操作(最初のものを除く)の間に、UKR350及びLKR400の符号マー内容は1又は2ビット位置だけシフトされる。各レジスタは所定のシフト時間に従つて、符号化プロセスの間に常に28ビット位置シフトされるので、この手順は符号マー・ビットの位置を並列を確保に行なわせるものである。

符号化操作の最初の読み出しにおいては、リセット200に含まれるメッセージ・ブロックの第1半分(32ビット)データ・ビットを含み、これらは各

4個のデータ・ビットより成る8個のセグメントとみなされる。各々6位のデータ・ビットを含む8個のセグメントを形成する48位のデータ・ビットへ組みられる。この結果、8位の4ビット・セグメントの各々のエンド・ビットを二進法することにより複数される。構成された48位のデータ・ビット(8位の6ビット・セグメントを形成するものと見えられる)は、8個のモジュロ2加算器500～514へ並列に印加される。各モジュロ2加算器は6個の並列的オフセットにより取つてある。これと同時に、56位の符号マー・ビットのうち、UKR350から送られた24位のマー・ビット及びLKR400から送られた24位のマー・ビットよりなる48位の並列の符号マー・ビットは、Pボンクス450において解説部(一定)された後、8個の6符号マー・ビット・セグメントとして、8個のモジュロ2加算器500～514の並列的オフセットへ並列に印加される。8位のモジュロ2加算器500～514は、8位の6ビット・セグメントを形成する

ものと見えられる複数された48位のデータ・ビットと、同じく8個の6ビット・セグメントを形成するものと見えられる複数された48位の符号マー・ビットとを並列的に組合せて、8位の並アフィン変換機能がシグナス以下、Pボンクスという)550～564のための選択の引数を構成する8個の6ビット・マスクメントを出力する。各Pボンクスは詳細な実験を実行する。各Pボンクスにおいては、先行の6ビット・データ・セグメントの二進にされた1エンド・ビット及び既定された1符号マー・ビットのモジュロ2加算と、次行の6ビット・データ・セグメントの二進にされた1エンド・ビット及び別の既定された1符号マー・ビットのモジュロ2加算との結果として生じた6ビット・セグメントの2エンド・ビットが形成されて、Pボンクス内の既定専用記憶装置(8位)に含まれる4位の16エントリー個性テーブルのうちの1つが選択される。各エントリーは4ビットから成つてゐる。次に、選択された複数テーブルにおける16個の9ビット・エントリー

のうちの1つが、構成された6ビット・セグメントの残り4ビットを解説することにより選択される。8個のPボンクスは並列に動作をつけており、次つて8個の6位をつた変換機能が実行されて、32ビットよりも1位の代号を決定する8個の4ビット・セグメントが与えられる。次いで、これらの32ビットはPボンクス600において、各々に與へられた順序による順序変換を受ける。このより本解説部及び他の解説の組合せにより、メッセージ・ブロックの第1半分に対する32ビットの該ブロック符号が生成される。この該ブロック符号は、モジュロ2加算器650～664へ印加される。もし且250にあるメッセージ・ブロックの第2半分の32データ・ビットもモジュロ2加算器650～664へ印加される。モジュロ2加算器650～664は、メッセージ・ブロックの第1半分に対するPボンクス600からの32ビットの該ブロック符号に従つて、もし且500からのメッセージ・ブロックの第12ビットを重複する。この結果、メッセージ・ブロ

クの変更された第2半分を被ねず新しい32ビットの軸を構成する8個の4ビット・グループが与えられる。メッセージ・ブロックの変更された第2半分の32ビットは、メッセージ・ブロックの第1半分を含んでいたUDR200へ印加され。これと同時に、メッセージ・ブロックの第1半分は、第2半分を含んでいたLDR250へ印加される。かくすることにより、メッセージ・ブロックの第1半分及び第2半分の互換が実現される。

暗号化プロセスの次の段階においては、URK350及びLKR400に記述されている暗号キーが、所定のシフト引数に従つてシフトされ。これにより新しい暗号キー・ビットの軸が供給される。次に、URK200に記述されているメッセージ・ブロックの変更された第2半分の32ビットが、同の本体ブロック暗号操作において、新しい暗号キー・ビットの軸と共に使用される。モジュロ2加算器650～664は、この本体ブロック暗号処理の結果に応じて、LDR250に記述されているメッセージ・ブロックの第1半分の3

2ビットを復元する。この変更された第1半分の32ビットは、メッセージ・ブロックの変更された第2半分の32ビットを配体していたURK200へ印加され。これと同時に、変更された第2半分の32ビットは、メッセージ・ブロックの第1半分の32ビットを配体していたLDR250へ転送される。

複数の軸出しを駆く複数の各機返し動作時においては、URK350及びLKR400にある暗号キー・ビットは、所定のシフト引数に従つてシフトされ、LDR250に記述されているメッセージ・ブロックの変更された半分(32ビット)は、URK200に記述されているメッセージ・ブロックの前に変更された半分の32ビットの軸ブロック軸に従つて再変更され、そしてモジュロ2加算器650～664からの再変更された半分は、既に変更された他の半分を配体していただDR200へ印加され。これと同時に、この他の方の半分はLDR250へ転送されて、メッセージ・ブロックの第1半分及び第2半分の互換が行

なわれる。

複数の転送し動作時には、URK350及びLKR400にある暗号キー・ビットは、所定のシフト引数に従つて成長シフトされて、供給された複数の暗号キー・ビットの軸が生成され。しりとり250に記述されている32ビットの変更された半分に対する複数の再変更が、URK200に記述されている前回変更された半分の32ビットの軸ブロック軸に従つて実行される。しかしながら、モジュロ2加算器650～664からの再変更された半分及びUDR200に記述されている前に変更された半分は互いに変換されることなく、元のメッセージ・ブロックに対する64ビットの軸変換されたブロックを構成する。16回目の軸出し後、UDR200の32ビットの内容及びモジュロ2加算器650～664の32ビット軸(これらは一れにまとめて、軸変換されたデータ・メッセージ・ブロックを表す)は、上部出力バッファ(UOB)700及び下部出力バッファ(LOB)750へ各自転送される。次い

で、UOB700に記述されている暗号化された4個の8ビット・ペイトのデータ及びLOB750に記述されている暗号化された4個の8ビット・ペイトのデータで構成される64ビットの暗号化されたデータ・ブロックは、8ビット・ペイト単位の並列・單列交換を行。一時に1ペイトずつPボンクス800へ充填される。64ビットの暗号化されたデータ・メッセージ・ブロックを完全に転送し終るためには、8サイクルが必要である。暗号化されたデータの各ペイトは、受信局への伝達のために、暗号化されたデータ・ビットをデータ・バス・アウトの並列なビット群へ映射すべく、Pボンクス800において複数の軸転換を受ける。

受信局においては、同じ暗号キーの割当のもとに同様を16回の転送し動作を実行することにより、64ビットの暗号化されたデータ・メッセージ・ブロックが解読される。しかしながら、暗号化プロセスの時とは異なり、解読プロセスに先立つURK350及びLKR400の暗号キー内容

暗号化操作における符号マー・ピントの選択を並列を複数行なわせると共に、別の解説プロセスに別する構造ができる。

本発明に従う暗号装置の詳細は第34～35図に示されており、次にこれらの図並びに第7～9図及び10図のタイミング図を参照して、より詳細な説明を行なうが、その前に、本発明の暗号装置で使用されるラシチ回路の具体例について、第4図を参照してお附しておく。ラシチ回路10は、4つのタイミング・クロンタで動作されるダイナミックFET回路によつて実現することができる。各クロンク相は、例えば250ナノ秒の持続時間を持つており、この場合、完全な1クロンク・サ・1クルは1～1クロクとなる。基本ラシチ回路は、正電極と負28との間に接続され、ゲート電極に複数のクロック信号11が印加される素子22と、負28及び29の間に並列的に接続され、各々のゲート電極に入力D3及びG3並びに入力D4及びG4が印加される2対の素子23及び24並びに25及び26と、素子29及び接地間に接続され、

の事前シフトは行なわれない。解説プロセスの場合と最初のものを聞くにあひては、UKR350及びLKR400の暗号キー内各は、暗号化プロセスの時と同じく、所定のソフト計画に従つて、1又は2ビット位置だけシフトされるか、暗号化プロセスを逆にして、その時実行されたすべての暗号化を元に戻すため、暗号キーのソフト万回は暗号化プロセスの時とは反対にされる。かくすることにより、元の64ビットのメッセージ・ブロックと同一のメッセージ・ブロックが再生される。また、解説プロセスの暗号化操作中に、UKR350及びLKR400の暗号キー内各は27ビット位置シフトされる。従つて、UKR350及びLKR400の暗号キー内各は28ビットのソフト・レジスターであるから、解説プロセスの終りにおいて、UKR350及びLKR400の暗号キー内各は、既に1ビット位置だけ移位シフトされる。この結果、暗号キーは所定のソフト計画に従つて、UKR350及びLKR400において完全に1回転シフトされることになり、解説プロセスの各

ゲート電極に複数のクロック信号11が印加される素子30と、正電極及び接地間に接続され、各々のゲート電極が複数のクロック信号11と、負28及び複数のクロック信号11に接続された3個の並列接続素子32、33及び34とを有している。素子32及び33間の接続点は、ラシチ回路10の出力端子36へ接続されると共に、素子25のゲート電極へフィードバック接続されて、入力D4を与える。回路内の接続チャバシタンス及び接続チャバシタンスは、一まとめてしてチャバシタ31及び35として示されている。素子23及び24並びに25及び26はアンド回路として、素子28はドクト・オア手段として、そして素子34はインバータとして各自働く。

次に、第5図をも参照して、第4図のラシチ回路10の動作について説明する。ラシチ回路10が最初“0”状態にあるものとすると、クロック信号11が印加されると、素子22がターン・オンされた時には、素子28は正電極の電位まで亢進される。この時、クロック信号11は印加されてい

ないので、素子30はカント・オノ状態に保たれており、従つて素子28の電位は暗黒に行なわれる。次に、クロック信号11が印加されると、素子28上の電荷は、入力D3及びD3又は入力D4及びD4へ印加される信号に応じて、そのまま保たれたり又は放電される。ラシチ回路10は0状態にあるものと仮定しているので、入力D4には低レベルの信号が印加されて、素子25を非活性に保ち、また入力G4にも低レベルの信号が印加されて、素子26を非活性に保つ。従つて、素子25、26及び30を介する放電路は働かない。素子23及び24を含む放電路に関しては、もし入力D3に“1”ビット（高レベル信号）が印加され、且つこれと同時に入力D3にゲート信号（高レベル信号）が印加されると、素子23及び24は共に切られ、素子30を介する放電路を形成し、その結果、素子28上の電荷は接地電位の方へ放電される。これに対し、入力D3に“0”ビット（低レベル信号）が印加されていると、たとえ入力D3にゲート信号が印加されても、クロック信号11

の間素子 2 3 は非導通に保たれるので、駆 2 8 から素子 2 4 及び 3 0 を介して基地に至る放電路は働かず、従つて高レベルの信号が駆 2 8 上に保持される。

次に、素子 3 2 のゲート電極へクロック信号 3 が印加されると、この時はまだクロック信号 4 が印加されていないので、素子 3 4 は非導通に保たれており、従つて駆 3 6 は正電位の電位まで充電される。次に、素子 3 4 のゲート電極へクロック信号 4 が印加されると、駆 5 6 上の動作は、駆 2 8 上の信号のレベルに応じてそのまま保持されるか又は放電される。もし駆 2 8 上に "1" ピントのデータ入力を探わす低レベルの信号が存在すると、クロック 4 の間素子 3 3 は非導通に保たれ、従つて駆 3 6 から素子 3 4 を介して基地に至る放電路は働かず、駆 5 6 上には "1" ピントの存在を探わす高レベルの信号が保持される。入力 4 3 に新しい入力信号が印加されない限り、ゲート信号 4 は低レベルにまづゲート信号 4 は高レベルに保たれるので、ランチ回路 1 0 が "1"

ピント状態にセットされた後は、素子 2 5 及び 2 6 のゲートに高レベルの信号が印加され、従つて次の 1/2 クロック時に素子 2 5 、 2 6 及び 3 0 を介する放電路が働いて、駆 2 8 を低レベルに保つ。これにより素子 3 3 は非導通に保たれるので、素子 3 4 を介する放電路は働かず、かくして駆 3 6 は、次の新しいデータ入力が印加されて、駆 5 6 に示されるようなゲート信号 4 及び 4 が印加されるまで高レベルに保たれる。これに対して、"0" ピントのデータ入力の結果として、駆 2 8 上に高レベルに信号が存在すると、クロック 4 の印加時に素子 3 3 が導通して、素子 3 4 を介する放電路を形成し、その結果、駆 5 6 上には "0" ピントの存在を探わす低レベルの信号が保持される。この場合、入力 4 4 に低レベルの信号が印加されることになるので、素子 2 5 は非導通に保たれ、従つて駆 2 8 に対する放電路は形成されない。このため、駆 2 8 上には電荷取扱高レベルの信号が保持される。この状態はまた素子 3 3 を導通状態に保ち、これにより素子 3 4 を介する放電路が

維持されて、駆 3 6 を低レベルに保つ。かくして、ランチ回路 1 0 の出力において最初データが確実に保たれる。

ランチ回路 1 0 が "1" 状態にある場合にも、クロック・サイクルは素子 2 2 へのクロック信号 4 1 の印加によつて開始される。前と同様に、素子 2 2 はクロック 4 1 の印加により導通して、駆 2 8 を正電位の電位まで充電させる。次に、クロック信号 4 2 が印加されると、駆 2 8 上の動作は、入力 4 3 及び 4 3 又は入力 4 4 及び 4 4 に印加されている信号のレベルに応じて、そのまま保持されるか又は放電される。もし入力 4 3 に "1" ピントのデータが印加されると、駆 2 8 上には低レベルの信号が保持され、一方入力 4 3 に "0" ピントのデータが印加されると、高レベルの信号が保持される。次に、素子 3 2 のゲート電極へクロック信号 4 3 が印加されると、この時クロック信号 4 4 がまだ印加されていないので、素子 3 4 は非導通に保たれ、従つて、駆 3 6 は正電位の電位まで充電される。次に、素子 3 4 のゲート電極へ

クロック信号 4 4 が印加されると、駆 3 6 上の動作は、駆 2 8 上の信号のレベルに応じて、そのまま保持されるか又は放電される。前に説明したように、"1" ピントのデータ入力の結果として、駆 2 8 上に低レベルの信号が存在すると、駆 3 6 上には高レベルの信号が保持されて、"1" ピントの存在を探わし、一方、"0" ピントのデータ入力の結果として、駆 2 8 上に高レベルの信号が存在すると、駆 3 6 上には低レベルの信号が保持されて、"0" ピントの存在を探わす。

ランチ回路 1 0 は、入力 D 1 及び G 1 に各々接続された素子 1 0 及び 1 9 を使用することによつて、2 ウエイ入力へ接続することができる。更に他の入力 D 2 及び L 2 に各々接続された素子 2 0 及び 2 1 を使用することによつて、3 ウエイ入力へ接続することもできる。以下で詳細に説明する本発明の実施例においては、1 ウエイ入力、2 ウエイ入力又は 3 ウエイ入力のランチ回路が本発明に応じて使用される。

まず駆 3 0 図に示されるように、8 バイトから

る 64 ビットのデータ・メッセージ・ブロックは、データ・バス・インを介して一時に 1 バイトずつ P ポンクス 50 へ印加される。各ビットは P ポンクス 50 において初期置換を受け、奇数番目 (0, 2, 4, 6) のデータ・ビットより既に組み込まれた奇数番目 (1, 3, 5, 7) のデータ・ビットより取る並に分割される。奇数番目の場合は LIB 100 へ送られ、一方、奇数番目の場合は LIB 150 へ送られる。LIB 100 は 4 個の 8 ビット・レジスタ U1B, U1I, 2U1B 及び 3LIB で構成され、LIB 150 も同様に 4 個の 8 ビット・レジスタ U1B, 1LIB, 2LIB 及び 3LIB で構成される。第 3 図には、奇数番目の最初及び最後のみが詳細に示されているが、偶のシフト・レジスタもこれと同じ構造である。

第 7 図のタイミング図を併せて参照するに、サイクル 0 において、1 つの有効データ・ビットが P ポンクス 50 を介して、LIB 100 及び LIB 150 へ印加されている時に、タイミング及

び制御信号 60 から LIB (G3) 及び LIB (G4) 軸へ信号が印加されて、最初の 8 ビット・ビットが、LIB 100 及び LIB 150 の各ソフト・レジスタの最初の段のランプ (例えば 102) へロードされる。メッセージ・ブロック山なりの 8 ビット・ビットは、後続のサイクル 1 から 7 までの間に、一時に 1 バイトずつ LIB 100 及び LIB 150 へ印加される。この場合、ビットの各ビットは、各ソフト・レジスタの最初の段 (03) へ印加される。LIB 及び LIB 軸上の信号は、シフト・レジスタの各段へ印加されるので、サイクル 1 乃至 7 の各々において、データ・ビットは各シフト・レジスタ内で 1 ビット位置ずつシフト・ダウンされ、従つてサイクル 7 の終了時には、LIB 100 及び LIB 150 は、供給されたデータ・メッセージ・ブロックを半分ずつロードされている。LIB 100 及び LIB 150 は直列・並列変換を実行し、その結果、LIB 100 及び LIB 150 へ逐次に供給された 8 ビットのメッセージ・ブロックは、これらの出

力において、各々 32 ビットより成る 2 つのダブループ (メッセージ・ブロックの第 1 半分及び第 2 半分) へ形成される。

次いで、第 3a, 3b 及び 3c 図を参照するに、64 ビットのメッセージ・ブロックが LIB 100 及び LIB 150 へ受取られて、そこにハンプアされている間に、64 ビットの外部レジスタからキー・バス・インを介して、暗号キーが一時に 7 ビット・ビットずつ P ポンクス 300 へ逐次に印加される。各 7 ビット・ビットは P ポンクス 300 で初期置換を受け、最初の 4 キー・ビット及び既り山 3 キー・ビットへ分割される。最初の 4 キー・ビットは UKR 350 へ印加され、一方、既りの 3 キー・ビットはビット位置を逆にして LKR 400 へ印加される。UKR 350 は 5 個の 8 ビット・レジスタ U1KR, 1UKR 及び 2UKR 及び 1 個の 4 ビット・レジスタ 3UKR で構成され、同様に LKR 400 は 3 個の 8 ビット・レジスタ U1KR, 1LKR 及び 2LKR 及び 1 個の 4 ビット・レジスタ 3LKR についても、

構成される。シフト・レジスタ U1KR の 4 段目のランプ 390 の出力は、シフト・レジスタ 3UKR の 1 段目のランプ 402 の入力に接続されている。第 3a 図に詳細に示されているように、8 ビット・レジスタ U1KR の第 1 段は 3 ウエイ入力ランプ 352 で構成され、他の段は第 2 段及び最終の段のランプ 354 及び 366 の如き 2 ウエイ入力ランプで構成される。8 ビット・レジスタ 1UKR 及び 2UKR もこれと同じ構成である。4 ビット・レジスタ 3UKR については、第 3a 図に示されるように、第 1 段は 3 ウエイ入力ランプ 384 で構成され、他の各段はランプ 390 の如き 2 ウエイ入力ランプで構成される。第 3b 及び 3c 図に示されるように、第 1 段は 3 ウエイ入力ランプで簡単な示されている LKR 400 の 8 ビット・レジスタ U1KR, 1LKR 及び 2LKR は、UKR 350 の対応するロジック・シフト・レジスタ U1KR, 1UKR 及び 2UKR と同じ構成を有している。第 3d 図に示される 4 ビット・レジスタ 3LKR については、その第 1 段は、シフト・レジスタ 3UKR の最前

後のラック390の出力に接続された3ワエイ入力ランプ402で構成され、他の各段は最終段のランプ408の取り2ワエイ入力ランプで構成される。かくして、UKR350及びLKR400の組合わせば、暗号キー・ワードのマー・ピントを記憶するための7個の8ビット・レジスタから成っているものとみなすことができる。

次に、第7回図も参照して、暗号キーのロード動作について説明する。サイクル0において有効暗号キー・マー・ピントかPランプス300を介してUKR350及びLKR400へ印加される時、ソフト・レジスタ0UKR, 1UKR, 2UKR, 3UKR, 0LKR, 1LKR及び2LKRの第1段に接続されたLDK(G3)線及びLDK(G4)線へ信号が印加され、これにより最初の7ピント・マー・ピントがUKR350及びLKR400の7個の各シフト・レジスタの第1段、例えば入力ランプ552, 568及び584などへロードされる。

サイクル1においては、暗号キーの2番目の7

ビット・マー・ピントか、UKR350及びLKR400の7個のシフト・レジスタの第1段へロードされる。これと同時に、各第1段の以前の内容即ち暗号キーの最初の7ピント・マー・ピントは、シフト・レジスタ0UKR, 1UKR, 2UKR, 3UKR, 0LKR, 1LKR及び2LKRの第2段に接続されている8R(G3)線及びLDK(G3)線への信号印加により、各々1ピント位置だけシフト・ダクションされる。各段のランプ内部の分解時間(resolution time)は、前段のランプの出力に変化が生じる直後でシフト動作を行なわせるのに十分なものである。

サイクル2においては、暗号キーの3番目の7ピント・マー・ピントが、UKR350及びLKR400の7個のシフト・レジスタの第1段へロードされる。これと同時に、第1段及び第2段の以前の内容即ち暗号キーの2番目及び最初の7ピント・マー・ピントは、シフト・レジスタ0UKR, 1UKR, 2UKR, 3UKR, 0LKR, 1LKR及び2LKRの第2段及び第3段に接続されている8R

線及びLDK(G3)線への信号印加により、各々1ピント位置だけシフト・ダクションされる。

サイクル3及び4においては、暗号キーの4番目及び5番目の7ピント・マー・ピントが、7個のシフト・レジスタの第1段へ依次にロードされ、これと同時にその内容は1ピント位置ずつシフト・ダクションされる。しかしながら、シフト・レジスタ3UKRの最軽段にあるピントは、サイクル4Rにおいてシフト・レジスタ3LKRの第1段へシフトされる。強制のサイクル5, 6及び7においては、暗号キーの残りの7ピント・マー・ピントか、シフト・レジスタ0UKR, 1UKR, 2UKR, 3UKR, 0LKR及び2LKRの第1段へ一時的に1ピントずつロードされる。LDK(G3)線及びLDK(G4)線上の信号は、各シフト・レジスタの第1段へ印加され、一方、8R線及びLDK(G3)線上の信号は、各ノット・レジスタの残りの段へ印加されるので、サイクル5, 6及び7の各々においては、暗号キー・ピントは1ピント位置ずつシフト・ダクションされ、従つてサイクル7の終了時には、UKR350及

びLKR400は暗号キーの第1半分及び第2半分を再ロードされている。

暗号キーのロード動作においては、UKR350及びLKR400は選列-並列並みを行ない、従つてUKR350及びLKR400に記憶されている暗号キーの8個の7ピント・マー・ピントは、各々28ピントよりなる2組の並列グループとして考えることができ。下記の表1及び表2は、UKR350及びLKR400へ暗号キーをロードする際のマー・ピントのマッピングの様子を示したものである。

特開昭51-108701(3)

表 3 図に示される UDR 200 及び LDR 250 は、各々 32 段のランチ 0 UDR-31UDR 及び 0 LDR-31LDR で構成される。第 2 図に示されるよう UDR、LDR 各々 16 段のデータ・ビット及び LDR 総へ信号が印加され、これにより UDR 100 及び LDR 150 にある 32 段のデータ・ビット及び LDR 150 にある 32 段のデータ・ビットが、各々 UDR 200 及び LDR 250 へ並列的に転送される。メッセージ・ブロックの 64 ビットは、下記の表 3 及び表 4 に示される如くに、UDR 200 及び LDR 250 へ分配される。

表 1
UKR のビット位置

	符号キー・ビット							
UKR 0 - UKR 7	56	48	40	32	24	16	8	0
UKR 8 - UKR 15	57	49	41	33	25	17	9	1
UKR 16 - UKR 23	58	50	42	34	26	18	10	2
UKR 24 - UKR 31	59	51	43	35				

表 2
LKR のビット位置

	符号キー・ビット							
LKR 0 - LKR 7	62	54	46	38	30	22	14	6
LKR 8 - LKR 15	61	53	45	37	29	21	13	5
LKR 16 - LKR 23	60	52	44	36	28	20	12	4
LKR 24 - LKR 31	27	19	11	3				

表 3
UDR のビット位置

	データ・ビット							
UDR 0 - UDR 7	56	48	40	32	24	16	8	0
UDR 8 - UDR 15	58	50	42	34	26	18	10	2
UDR 16 - UDR 23	60	52	44	36	28	20	12	4
UDR 24 - UDR 31	62	54	46	38	30	22	14	6

表 4
LDR のビット位置

	データ・ビット							
LDR 0 - LDR 7	57	49	41	33	25	17	9	1
LDR 8 - LDR 15	59	51	43	35	27	19	11	3
LDR 16 - LDR 23	61	53	45	37	29	21	13	5
LDR 24 - LDR 31	63	55	47	39	31	23	15	7

表 7 図に示されるように、LDR 総へこれら以上信号は出力されない。併せて、シフト・レジスタ 3 UKR の最初のランチ 390 からシフト・レジスタ 3 LKR の最初のランチ 400 に掛けるか続行以後使用されず、これらの間では如何なるビット転送も行なわれない。シフト・レジスタ 3 UKR の最初のランチ 390 の出力は、シフト・レジスタ 0 UDR の第 1 故のランチ 352 に記録され、シフト・レジスタ 3 LKR の最初のランチ 400 の出力は、シフト・レジスタ 0 LDR の第 1 故のランチ (表示せず) に記録されているので、UKR 550 及び LKR 400 は、各々独立した 28 ビットのシフト・レジスタと見えることができる。UKR 550 及び LKR 400 に記録されている符号キー・ビットは、符号化プロセスに先立つて 1 ビット位置ずつ串列シフト・アシブされる。この場合、UKR 550 の第 1 故のランチ 352 に記録されていたビットは、UKR 550 の最初のランチ 390 へ接続シフトされ、同様に、LKR 400 の第 1 故のランチに記録さ

れていたビットは、 L K R 4 0 0 の最初のランチ 4 0 8 へ領域シフトされる。このような事前シフトは、 マイクル8において、 U K R 3 5 0 及び L K R 4 0 0 のすべての段に実現されている S L か及び L D K かへ移行を加ることにより行なわれる。各ランチの出力は前段のランチへ転写されており、 かつて、 S L か及び L D K かへの信号印加により、 各ランチから前段のランチへキー・ビットが転送される。例えば、 これらの信号印加によってランチ 3 5 4 のビット内容をランチ 3 5 2 へ有効にシフトさせるため、 ランチ 3 5 4 の出刀 U K R 1 はランチ 3 5 2 の 1 入力に接続されている。同様に、 ソンチ 3 5 2 のビット内容をランチ 3 9 0 へ有効にシフトさせるため、 ランチ 3 5 2 の出刀 U K R 0 はランチ 3 9 0 の 1 入力に接続されている。暗号化プロセスの開始前に行なわれるこのような暗号キー・ビットの事前シフトは、 暗号化プロセスの最初の翻訳しにおけるキー・ビットの適切な排列を確実にするものである。暗号化プロセスに入ると、 U K R 3 5 0 及び L K R 4

0 0 にある暗号キー・ビットを常に 2 7 ビット位
置シフトさせるため、 最初の翻訳しを除く各翻
訳しの U K C 、 U K R 3 5 0 及び L K R 4 0 0 は 1 段
は 2 ビット位置ずつシフトアップされる。U K
C 3 5 0 及び L K R 4 0 0 は共に 2 8 ビットのシ
フト・レジスタであるから、 これらに記憶されて
いる暗号キー・ビットの 2 8 ノット。即ち、 1 翻
訳シフト及び暗号化プロセスにおける 2 7 ビット
は、 暗号化プロセスの開始時と同じ、 翻訳し操作
の右に暗号キー・ビットを適切に並列させるもの
である。下記の表 5 は、 順序キーに対する所定の
シフト時間示したものである。

暗号キーのシフト時間

暗号化 (シフト・アップ) (順序シフト)	暗号化 (シフト・ダウン) (シフト・ダウン)																4 (順序シフト)
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	4 (順序シフト)

れていたビットは、 LKR400 の最終段のランテ408へ微減シフトされる。このような事前シフトは、 サイタル8Kにおいて、 UKR350 及び LKR400 のすべての段に実現されているとし て及び LDK へ倍率を印加することにより行なわれる。各ツチの出力は前段のランテへ接続さ れており、 例へ、 9L解説及び LDK 説への信号印加により、 各ツチから前段のツチへキー・ ビントが転送される。例えば、 これらの信号印加によつてランテ354 のビント内容をランテ352 へ有効にシフトさせるため、 ランテ354 の出 力 LKR1 はランテ352 の1入力に接続されて いる。同様に、 ランテ352 のビント内容をランテ390 へ有効にシフトさせるため、 ランテ352 の出力 LKR0 はランテ390 の1入力に接続さ れている。暗号化プロセスの開始前に行なわれ るこのような暗号マー・ビントの事前シフトは、 暗号化プロセスの最初の転送におけるキー・ビントの適切な並列を確実にするものである。暗号 フロセスに入ると、 UKR350 及び LKR4

00 にある暗号マー・ビントを常に27ビント位 ソシフトさせるため、 最初の転送を除く各転送 しの間に、 UKR350 及び LKR400 は1又 は2ビント位置ずつシフト・アンプされる。 UKR350 及び LKR400 は共に28ビントのノ ート・レジスターであるから、 これらに記憶さ れている暗号マー・ビントの2ビント、 即ち、 1事 前シフト及び暗号化プロセスにおける27シフト は、 暗号化プロセスの開始時と同時に、 転送し取作 の前に暗号マー・ビントを適切に並列させるもの である。下記の表は、 暗号マーに対する所定の シフト計画を示したものである。

暗号マーのシフト計画

転送し暗号	暗号化 (シフト・アダプ)		解読 (シフト・アダプ)	
	（事前シフト）	1	（事前シフト）	1
1	1	2	2	2
2	2	3	3	3
3	3	4	4	4
4	4	5	5	5
5	5	6	6	6
6	6	7	7	7
7	7	8	8	8
8	8	9	9	9
9	9	10	10	10
10	10	11	11	11
11	11	12	12	12
12	12	13	13	13
13	13	14	14	14
14	14	15	15	15
15	15	16	16	16
16	16			

表5中の“1”は、U KR 350 及び L KR 400における1ビット位置のシフトを表わし、“2”は2ビット位置のシフトを表わす。

暗号化プロセス

本説明に従う暗号装置を使用する暗号化プロセスは、16回の繰返し操作によつて、データ・ビットのメッセージ・ブロックを暗号化する。

U KR 350 及び L KR 400 にあるキー・ビットの初期シフトは、暗号化プロセスの開始時に、サイクル8において実行される。これは、U KR 350 及び L KR 400 のすべての段に分配されている S L 線及び L DK 線へ最初の信号を追加することによって行なわれ、暗号キーは1ビット位置だけシフト・アップされる。この結果、サイクル8の終了時には暗号化プロセスの最初の繰返し操作のための暗号キー・ビットの最初の組が与えられる。暗号化プロセスの最初の繰返し操作は、サイクル9及び10で実行され、U KR 350 にある28個の初期シフトされた暗号キー・

表題 第5-108709(15)
ビットのうちの24ビット及び L KR 400 における28個の初期シフトされた暗号キー・ビットのうちの24ビットを P ポンクス 450 で並形置換することにより開始される。P ポンクス 450 は、下記の暗号キー・ビットのマッピングを示す表及び7に従つて、U KR 350 及び L KR 400 からの48ビットの任意に決められた順序を行なう。

表 6
暗号キー・ビットの意味マップ

ビット番号	割り当たしたビット番号
U KR 0	U KR 13
U KR 1	U KR 16
U KR 2	U KR 10
U KR 3	U KR 23
U KR 4	U KR 0
U KR 5	U KR 4
U KR 6	U KR 2
U KR 7	U KR 27
U KR 9	U KR 14
U KR 10	U KR 4
U KR 11	U KR 20
U KR 12	U KR 7
U KR 13	U KR 27
U KR 14	U KR 12
U KR 15	U KR 11
U KR 16	U KR 7
U KR 18	U KR 25
U KR 19	U KR 7
U KR 20	U KR 15
U KR 22	U KR 6
U KR 23	U KR 26
U KR 25	U KR 10
U KR 26	U KR 17
U KR 27	U KR 1

表 7
暗号キー・ビットの意味マップ

ビット番号	割り当たしたビット番号
L KR 0	L KR 12
L KR 1	L KR 23
L KR 2	L KR 2
L KR 3	L KR 8
L KR 4	L KR 18
L KR 5	L KR 26
L KR 7	L KR 1
L KR 8	L KR 11
L KR 10	L KR 22
L KR 11	L KR 16
L KR 12	L KR 4
L KR 13	L KR 19
L KR 15	L KR 15
L KR 16	L KR 20
L KR 17	L KR 10
L KR 18	L KR 22
L KR 19	L KR 5
L KR 20	L KR 24
L KR 21	L KR 17
L KR 22	L KR 13
L KR 23	L KR 21
L KR 24	L KR 7
L KR 26	L KR 0
L KR 27	L KR 3

8個の6ビント・マクメントと薄えられる48個の置換された暗号キー・ビントは、各々6個の階級的オア回路（第3セ、51及び38回路X0Rで示されている）より成る8個のモノユロ2加算器500、502、504、506、508、510、512及び514へ1入力として印加される。これと同時に、UDR200に含まれる32データ・ビントより取り且つ8個の4ビント・セグメントと考えられるメッセージ・ブロックの第1半分が、8個の6ビント・マクメントを解消する48個のデータ・ビントへ拡張されて、8個のモノユロ2加算器500～514の他の入力へ印加される。データ・ビントの拡張は、第5セ、51及び38回路に示されるように、8個の4ビント・セグメントの各々のエンド・ビント（図示の例では、各4ビント・セグメントの最初の2ビント）を二重にしてことによつて達成される。下記の表8及び表9に示されるように、8個のモノユロ2加算器500～514は、拡張された48個のデータ・ビント及び複数された48個の暗号キー

毎回 番51-108701(16)
一・ピントを総合力せて、B端の8ボックスから
手アフターで製版機能ボンクス5×0~5.64に対
する鏡面の引数を構成するが、いきなりの6ピント
・セグメントで出力する。

ビット数		ビット数		ビット数		ビット数		ビット数		ビット数	
個数	割合	個数	割合	個数	割合	個数	割合	個数	割合	個数	割合
UER 13	●	UEB 31	○	UEA 3	○	UEC 7	○	UEH 2	○	UEG 2	○
UEA 14	●	UEB 30	○	UEA 1	○	UEC 6	○	UEH 1	○	UEG 1	○
UEA 10	●	UEB 29	○	UEA 2	○	UEC 5	○	UEH 0	○	UEG 0	○
UEA 23	●	UEB 28	○	UEA 3	○	UEC 4	○	UEH 0	○	UEG 0	○
UEA 0	●	UEB 27	○	UEA 4	○	UEC 3	○	UEH 1	○	UEG 1	○
UEA 4	●	UEB 26	○	UEA 5	○	UEC 2	○	UEH 0	○	UEG 0	○
UEA 2	●	UEB 25	○	UEA 6	○	UEC 1	○	UEH 0	○	UEG 0	○
UEA 27	●	UEB 24	○	UEA 7	○	UEC 0	○	UEH 1	○	UEG 1	○
UEA 14	●	UEB 23	○	UEA 8	○	UEC 9	○	UEH 0	○	UEG 0	○
UEA 5	●	UEB 22	○	UEA 9	○	UEC 8	○	UEH 0	○	UEG 0	○
UEA 20	●	UEB 21	○	UEA 10	○	UEC 7	○	UEH 0	○	UEG 0	○
UEA 9	●	UEB 20	○	UEA 11	○	UEC 6	○	UEH 0	○	UEG 0	○
UEA 72	●	UEB 19	○	UEA 12	○	UEC 5	○	UEH 0	○	UEG 0	○
UEC 18	●	UEB 18	○	UEA 13	○	UEC 4	○	UEH 0	○	UEG 0	○
UEC 11	●	UEB 17	○	UEA 14	○	UEC 3	○	UEH 0	○	UEG 0	○
UEC 3	●	UEB 16	○	UEA 15	○	UEC 2	○	UEH 0	○	UEG 0	○
UEC 25	●	UEB 15	○	UEA 16	○	UEC 1	○	UEH 0	○	UEG 0	○
UEC 7	●	UEB 14	○	UEA 17	○	UEC 0	○	UEH 0	○	UEG 0	○
UEC 25	●	UEB 13	○	UEA 18	○	UEC 9	○	UEH 0	○	UEG 0	○
UEC 6	●	UEB 12	○	UEA 19	○	UEC 8	○	UEH 0	○	UEG 0	○
UEC 26	●	UEB 11	○	UEA 20	○	UEC 7	○	UEH 0	○	UEG 0	○
UEC 19	●	UEB 10	○	UEA 21	○	UEC 6	○	UEH 0	○	UEG 0	○
UEC 12	●	UEB 9	○	UEA 22	○	UEC 5	○	UEH 0	○	UEG 0	○
UEC 1	●	UEB 8	○	UEA 23	○	UEC 4	○	UEH 0	○	UEG 0	○

電極された ビット番号	ビット番号	オシロスコープ ビット番号	オシロスコープ ビット番号	オシロスコープ ビット番号
LBR 17	●	WDR 15	○	●
LBR 23	●	WDR 14	●	●
LBR 7	●	WDR 17	●	●
LBR 8	●	WDR 10	●	●
LBR 18	●	WDR 19	●	●
LBR 26	●	WDR 20	●	●
LBR 1	●	WDR 18	●	●
LBR 12	●	WDR 20	●	●
LBR 22	●	WDR 21	●	●
LBR 16	●	WDR 22	●	●
LBR 4	●	WDR 23	●	●
LBR 19	●	WDR 24	●	●
LBR 15	●	WDR 21	●	●
LBR 20	●	WDR 24	●	●
LBR 10	●	WDR 23	●	●
LBR 21	●	WDR 26	●	●
LBR 5	●	WDR 27	●	●
LBR 24	●	WDR 28	●	●
LBR 17	●	WDR 27	●	●
LBR 13	●	WDR 28	●	●
LBR 21	●	WDR 29	●	●
LBR 7	●	WDR 30	●	●
LBR 0	●	WDR 31	●	●
LBR 1	●	WDR 0	●	●

第3。図中の#09ボンクス550の計算を第6圖に示す。図示の如く、#09ボンクス550はデコード552及びR08584から成つている。この#09ボンクス550へは、#0モジユロ2加算部550からの6ピント・セグメントが入力として追加される。この6ピント・セグメントのエンド・ピント0及び5、即ち、二進にされた元データ・ピントUDR31及び置換された符号マー・ピントUKR73のモジユロ2加算と、二進にされたデータ・ピントUDR4及び置換された符号マー・ピントUKR4のモジユロ2加算とから生成されたピントを残ねず信号は、インパート554及び556へ各々印加され、これによりエンド・ピントの相殺信号が得られる。エンド・ピントのモジユロ2加算の結果が0である、各々16倍のアンド回路を含む4グループのうちの1つ、即ち、アンド回路568及び570を含む第1グループが選択される。同様に、エンド・ピントのモジユロ2加算の結果が01である、アンド回路572及び574を含む第2グループ

が選択され。結果が 1 0 であれば、アンド回路 6
7 6 及び 5 7 を暫時解きグループが選択され、
そして段階に結果が 1 1 であれば、アンド回路 5
8 0 及び 5 8 2 を含む第 4 グループが選択される。
サ 0 8 ポンクス 5 5 0 へ印加される 6 ピント・セ
グメントの内側の 4 ピント (1, 2, 3, 4) を
対応するインバータ 5 5 8, 5 6
0, 5 6 2 及び 5 6 4 へ各々印加され、これにより
内側 4 ピントの補助信号が生成される。6 ピント・セグメントの内側 4 ピントは、選択されたグ
ループに含まれる 16 個のアンド回路のうちの 1
つに上づて解説され、R 0 3 5 8 4 の肯定のアド
レス向へ出力信号を送る。R 0 8 5 8 4 は、基本
的には 4 個の複数テーブル即ち R 0 8, 1 R 0
8, 2 R 0 8 及び 3 R 0 8 で解説される。各複数
テーブルは、16 個のエントリーを有しており、
これらの中の各エントリーは、電子 5 8 6, 5 8 7,
5 8 8 及び 5 8 9 の如き 4 個の P B T 素子で実現
され得る 4 ピントから成っている。これらの素子
は、一旦選択されると、R 0 8 5 8 4 の出力線 5

8ビット暗記テーブル▲

94、595、596及び597へ一意的な4ビットコードを供給する。Cの4ビット・セグメントは、8ビットスケルの4本の出力番号、90、91、92及び93の方へ通られる。

23～38間に示される仙の74の8ビットスケル、552、554、556、558、560、562及び564も、高等的には408ビットスケルと同様な用法であるか。各8ビットスケルに含まれる機能テーブルは互いに異なつておらず、従つて各機能の名をつた説明欄が与えられる。下記の表10、11、12及び13は、8個の8ビットスケル(番号～#7)の機能テーブルのは力を示すもので、各出力を表わす10進数は、実際には4ビットの2進数ターン(例えば10101110など)で出力される。

8ビットスケル内部ビット	#08ビットスケル				#18ビットスケル			
	00	01	10	11	00	01	10	11
0000 (0)	14	0	4	13	14	3	0	13
0001 (1)	4	15	1	12	1	13	14	8
0010 (2)	13	7	14	9	8	4	7	10
0011 (3)	1	6	9	2	14	7	13	1
0100 (4)	3	14	13	4	6	15	10	3
0101 (5)	14	2	6	9	11	2	4	15
0110 (6)	11	13	3	1	3	8	13	4
0111 (7)	0	3	11	7	4	14	1	2
1000 (8)	3	10	13	5	9	12	5	11
1001 (9)	10	6	12	11	2	0	6	6
1010 (10)	6	12	9	1	2	1	12	7
1011 (11)	12	11	7	10	15	10	6	12
1100 (12)	6	9	3	10	12	6	8	0
1101 (13)	0	5	10	0	0	9	3	5
1110 (14)	0	3	5	4	5	11	2	14
1111 (15)	7	8	0	13	20	5	15	9

表 11

8ビット暗記テーブルB

8ビット暗記ビット	#16ビットスケル							
	00	01	11	00	01	10	11	00
0000 (0)	10	13	11	1	7	13	10	3
0001 (1)	0	7	6	10	13	8	6	15
0010 (2)	9	0	4	13	14	11	9	0
0011 (3)	24	5	9	0	3	5	0	6
0100 (4)	6	3	8	6	6	12	20	
0101 (5)	3	4	15	9	6	15	11	1
0110 (6)	15	4	3	7	10	9	13	8
0111 (7)	5	10	0	7	10	9	13	8
1000 (8)	1	2	11	4	1	4	15	9
1001 (9)	13	8	1	15	2	7	1	4
1010 (10)	13	5	2	14	8	2	3	5
1011 (11)	7	14	12	3	5	12	14	21
1100 (12)	11	12	5	11	11	7	5	12
1101 (13)	1	11	10	5	12	10	2	7
1110 (14)	2	15	14	2	4	11	3	9
1111 (15)	8	2	7	27	15	15	16	9

智慧 8451—108701(19)

卷之三

日本サタクス社能サープル D

# 78-0708		# 68-0708		# 58-0708	
スケルトン	マスク	スケルトン	マスク	スケルトン	マスク
00000 [0]	00 01 29 32	00 01 10 15	00 01 10 15	00 01 10 15	00 01 10 15
00001 [1]	01 02 11 12	02 03 11 12	02 03 11 12	02 03 11 12	02 03 11 12
00010 [2]	02 03 11 12	03 04 12 13	03 04 12 13	03 04 12 13	03 04 12 13
00011 [3]	04 05 13 14	05 06 13 14	05 06 13 14	05 06 13 14	05 06 13 14
00010 [4]	05 06 13 14	06 07 14 15	06 07 14 15	06 07 14 15	06 07 14 15
00101 [5]	00 09 3 4	01 10 4 5	01 10 4 5	01 10 4 5	01 10 4 5
00110 [6]	00 01 7 10	01 02 7 10	01 02 7 10	01 02 7 10	01 02 7 10
00111 [7]	03 00 14 7	04 05 14 7	04 05 14 7	04 05 14 7	04 05 14 7
10000 [8]	03 04 10 9	04 05 10 9	04 05 10 9	04 05 10 9	04 05 10 9
10001 [9]	02 03 25 5	03 04 25 5	03 04 25 5	03 04 25 5	03 04 25 5
10010 [10]	09 05 6 0	10 06 6 0	10 06 6 0	10 06 6 0	10 06 6 0
10011 [11]	04 07 6 12	05 08 6 12	05 08 6 12	05 08 6 12	05 08 6 12
11000 [12]	05 02 0 14	06 03 0 14	06 03 0 14	06 03 0 14	06 03 0 14
10012 [13]	10 05 5 2	11 06 5 2	11 06 5 2	11 06 5 2	11 06 5 2
11100 [14]	06 03 3 12	07 04 3 12	07 04 3 12	07 04 3 12	07 04 3 12
11111 [15]	01 06 2 12	02 07 2 12	02 07 2 12	02 07 2 12	02 07 2 12

1

日本アラスカ根付チーブル

# 48.000.000	8.000.000	8.000.000	# 58.000.000
00 01 10 11	00 01 10 11	00 01 10 11	00 01 10 11
(01) (11)	(01) (11)	(01) (11)	(01) (11)
0000 (0)	2 14	4 11	12 10
0001 (1)	12 11	2 8	9 4
0010 (2)	6 2	1 12	15 14
0011 (3)	1 12	11 7	1 15
0100 (4)	7 4	10 1	2 12
0101 (5)	10 7	13 14	5 12
0110 (6)	11 13	7 2	9 11
0111 (7)	6 2	8 13	5 10
1000 (8)	8 5	15 6	6 7
1001 (9)	5 6	9 15	1 0
1010 (10)	3 15	17 0	3 11
1011 (11)	15 10	5 9	4 14
1100 (12)	13 3	6 10	8 1
1101 (13)	0 9	3 4	7 23
1110 (14)	14 3	0 5	3 3
1111 (15)	2 6	6 14	11 8

8個のSボックス550～564は、32ビットの代替グループを規定する8個の4ビット・セグメントを供給し、次いでこれらのセグメントは、Sボックス600において、任意に組み込まれる形によつて最終実現される。Sボックス550～564で実行される並列比較及びSボックス600で実行される順序変換の結果、メッセージ・ブロックの第1半分の新ブロック番号が生成される。下記の表14は、Sボックスの出力の順序解決の様子を示したものである。

表 14		Sボックス・セグメント番号	構成されたビット番号							
Sボックス出力の順序チャート										
S番	S番									S番
		S1	S2	S3	S4	S5	S6	S7	S8	
550	551	552	553	554	555	556	557	558	559	560
560	561	562	563	564	565	566	567	568	569	560
569	570	571	572	573	574	575	576	577	578	579
579	580	581	582	583	584	585	586	587	588	589
589	590	591	592	593	594	595	596	597	598	599
599	600	601	602	603	604	605	606	607	608	609
609	610	611	612	613	614	615	616	617	618	619
619	620	621	622	623	624	625	626	627	628	629
629	630	631	632	633	634	635	636	637	638	639
639	640	641	642	643	644	645	646	647	648	649

第3カ、31及び32図に示されるように、別の8例のモジュロ2加算器650、652、654、656、658、660、662及び664は、各々4例の並列的オブ回路XORで構成される。LDR250に保持されているメッセージ・ブロックの第2半分(32データ・ビットより成り、8個の4ビット・データ・セグメントと考えられる)は、メッセージ・ブロックの第1半分の並列プロセッタ信号を表わす複数された32ビットのグループと共に、これらのモジュロ2加算器650～664の入力へ印加される。モジュロ2加算器650～664は、これらの入力から、メッセージ・ブロックの変更された第2半分を表わす新しい32ビットのグループを構成する8個の4ビット・セグメントを生成し、次いでこの新しい32ビットのグループは、母線を介して第33図のUDR200へ転送される。

再び第33図及び第73図を参照するに、サイクル10の前半において、UDR200のすべてのランプに接続されているLB線及びLDK線へ

信号が印加され、これによりノンセグ・ブロックの変更された第2半分を表わす32ビットのグループがUDR200へロードされる。これと同時に、LB線及びLDK線上の信号は、LDR250のすべてのランプへも印加され、この結果、UDR200に記憶されていたメッセージ・ブロックの第1半分がLDR250のランプへ転送されて、そこに記憶される。メッセージ・ブロックの第1半分及び変更された第2半分のこのようない互換は、暗号化プロセスの次の繰返し操作を実行するための準備であり、これで、サイクル8における暗号キーの事前シフト後に開始された最初の繰返し操作が完了したことになる。

2回目の繰返し操作は、サイクル10、11及び12で実行され、サイクル10におけるシフト動作から開始される。最初のサイクル10の間に、Sレジ及びLDK線を介してRDR550及びLDR400のすべての端へ印加される第2信号により、暗号キーが更に1ビット位置だけシフト・アップされる。これは、暗号化プロセスの2回目

の繰返し操作に対する第2組の暗号キー・ビットを与えるものである。サイクル11においては、UDR200に記憶されているメッセージ・ブロックの変更された第2半分が、上述と同様な並列プロセッタ信号処理操作で使用され。次にその結果がモジュロ2加算器650～664で使用され、LDR250に記憶されているメッセージ・ブロックの第1半分が変更される。

サイクル12においては、UDR200のすべてのランプに接続されているLB線及びLDK線への第2信号の印加により、メッセージ・ブロックの変更された第1半分を表わす新しい32ビットのグループがUDR200に記憶される。これと同時に、LB線及びLDK線上の第2信号は、LDR250のすべてのランプへも印加され。これによりUDR200に記憶されていたメッセージ・ブロックの変更された第2半分がLDR250へ転送されて、そこに記憶される。この互換操作は、暗号化プロセスの次の繰返し操作するための準備であり、これで暗号化プロセスの2回目

の繰返し操作が完了される。

前述の表5の暗号キー・シフト計画に示されるように、暗号化プロセスの3回目の繰返し操作(サイクル11、12、13及び14で実行される)においては、暗号キーは2ビット位置だけシフトされねばならない。従つて、サイクル11の間にSレジ及びLDK線へ第3信号を印加することになり、暗号キーの2回のシフトのうちの最初のシフトが行なわれる。3回目の繰返し操作を実行するためのこの最初のシフト操作は、暗号装置内の分解時間の故に、Sレジへの第2信号の印加によって開始された2回目の繰返し操作に対して影響を及ぼさない。暗号キーは、サイクル12の間にSレジ及びLDK線へ印加される第4信号によつて、更に1ビット位置だけシフト・アップされる。このようだ、暗号キーは、3回日の繰返し操作の間にSレジ及びLDK線へ印加される第3信号及び第4信号により、2ビット位置だけシフト・アップされる。

暗号化プロセスにおける後続の繰返し操作も、

同様にしてまた暗号キーのシフト計画に従つて実行される。最後の転送し操作を除く残りの各操作においては、UKR350及びLKR400に記憶されている暗号キー・ピントは、所定のシフト計画に従つてシフトされ、LDR250に記憶されているメッセージ・ブロックの変更された半分は、UDR200に記憶されているメモセージ・ブロックの以前に変更された半分の横ブロック番号に従つて再変更され、そしてモジュロ2加算器650～664からのこの再変更された半分は、メモセージ・ブロックの以前に変更された半分に代つてUDR200へロードされ、これと同時に、UDR200に記憶されていたこの以前に変更された半分は、LDR250へ転送されて、その前の内容に代つてそこに記憶される。

サイクル38及び39で実行される暗号化プロセスの最後の転送し操作においては、UKR350及びLKR400に記憶されている暗号キー・ピントは、所定のシフト計画に従つて最終シフトされ、そしてLDR250に記憶されているメモ

セージ・ブロックの変更された半分に対する最後の再変更が、UDR200に記憶されているメモセージ・ブロックの以前に変更された半分の横ブロック番号に従つて実行される。しかしながら、サイクル39は降は、LB線上に信号が存在しないので、モジュロ2加算器650～664からの再変更された半分及びUDR200に記憶されている以前に変更された半分は互換されず、これらは元のメモセージ・ブロックの被暗号化ブロックを構成する。かくして、64ビットの被暗号化メッセージ・ブロックを扱わすUDR200からの32ビットの出力及びモジュロ2加算器650～664からの32ビットの出力は、対応するUOB700及びLOB750へ各自印加される。第38、39及び30図に示されるように、UOB700は4個の8段シフト・レジスタUOB、1UOB、2UOB及び3UOBで構成され、同様に、LOB750も4個の8段シフト・レジスタLOB、1LOB、2LOB及び3LOBで構成される。図面には、最初のシフト・レジスタ

0UOBの第1段(ランチ702)、第2段(ランチ704)及び最終段(ランチ716)のみが詳細に示されているが、残りの段及び他のシフト・レジスタもこれと同じ構成である。

次に、第70図をも参照して、これらのシフト・レジスタの動作について説明する。まずサイクル40において、UOB700及びLOB750の各シフト・レジスタのすべてのランチに接続されているLDOB線及びLDOD線へ信号が印加され。これによりUDR200からUOB700への32ビット出力の並列転送及びモジュロ2加算器650～664からLOB750への32ビット出力の並列転送が同時に実行される。

UOB700及びLOB750へロードされた64ビットの被暗号化ブロックは、そこで一時に8ビット・バイトずつ並列-直列変換を受け、各シフト・レジスタの最終段のビット内容が、1つの8ビット・バイトとしてPボンクス800へ印加される。Pボンクス800では、暗号化されたデータ・ビットをデータ・バス・アクトの通路な

ビット欄へ接続するために、各8ビット・バイトに対する最後の直列変換が行なわれる。UOB700及びLOB750における並列-直列変換は、8個の各シフト・レジスタUOB～3LOBの第2段から第8段までに、D0B線及びD1B線を介して信号を印加することによって実行され、かくして、サイクル41～47の間に、各シフト・レジスタにあるデータ・ピントが1ビット位置ずつシフト・ダウンされる。各々の最終段からのビットで構成された8ビット・バイトは、上述のようにPボンクス800で置換された後、データ・バス・アクトへ出力される。サイクル48において、64ビットの暗号化されたブロックの最後のバイトが転送され、これで暗号化プロセスが完了する。

第71及び72図には、次のメッセージ・ブロックを暗号化するためのサイクルは示されているが、暗号化されるべきメッセージ・ブロックがあと数つあつても、上と同じような方式で暗号化することができる。従つて、データの最初のメ

セージ・ブロックが暗号化されている間に、もし次のメッセージ・ブロックが暗号装置に受取られると、Cのメッセージ・ブロックはU1B100及びL1B150へロードされる。サイクル59が終つて、最初の暗号化プロセスの操作の繰返し操作が完了すると、暗号キーはUKR350及びLKR400内で完全に回転されて、元の状態に戻され、従つてデータの次のメッセージ・ブロックの暗号化を開始する準備ができる。最初の暗号化プロセスのサイクル40において、暗号化された最初のメッセージ・ブロックがU0B700及びL0B750へ転送されている間に、第7回に破壊で示されるように、1日T記号及びLDR記号へ信号を印加することにより、次のメッセージ・ブロックをUDR200及びLDR250へ転送することができ。そして次の暗号化プロセスは、最初のメッセージ・ブロックがU0B700及びL0B750からドボンクス800を介してデータ・バス・アウトへ転送されている間に、開始され得る。もし暗号装置に対するメッセージ・ブ

クタの伝送率が高くなり過ぎて、前のメッセージ・ブロックが入力バッファからデータ・レジスターへ転送されてしまう前に次のメッセージ・ブロックが受信されるようを状態が生じ得るならば、このような状態を知らせる(例えば、使用中信号を出す)ことのできる回路を設けなければならない。これは、後続のデータ・メッセージ・ブロックが暗号装置の動作速度において、同期的に伝送されるのを可能にする。

解説プロセス

本発明に使う暗号装置において、64ビットの暗号化されたデータ・メッセージ・ブロックを解説するための解説プロセスは、暗号化プロセスで使用されたのと同じ暗号キーの初期のもとに、何種か16回の繰返し操作を実行することによつて達成される。しかしながら、解説プロセスにおいては、暗号キーは、暗号化プロセスの場合のように、最初の操作前に最初シフトされるのではなく、最後の操作後に最後シフトされる。

更に、暗号キーは、前記の表5に示されるシフト計画に従つて、暗号化プロセスの時とは反対の方向にシフトされる。これは、暗号化プロセスにおいて実行されたすべての操作を元に戻して、元のメッセージ・ブロックと同一の64ビットのメッセージ・ブロックを再生するようだ。解説操作時ににおける暗号キー・ビットの適切な並列を確実に行なわせるものである。

図33～34図及び図7～8図を参照するに、前と同じようにサイクル0～7において、暗号化されたデータ・メッセージ・ブロックはデータ・バス・インを介して受信された後、U1B100及びL1B150へバックアラーム。そして暗号キーはUKR350及びLKR400へロードされる。次にサイクル8では、暗号化されたメッセージ・ブロックがU1B100からUDR200へ及びL1B150からLDR250へ各々並列に記憶される。暗号化プロセスの時と同様に、サイクル9において、UDR200に記憶されている暗号化されたメッセージ・ブロックの第1半分が、置

換された1組の暗号キー・ビットと共に複数ブロック暗号処理操作で使用され。その結果はモジュロ2加算器650～664へ送られて、LDR250に記憶されているメッセージ・ブロックの第2半分を変更するのに使用される。次のサイクル10では、UDR200へ印加される第1信号及びLDR250へ印加される信号により、暗号化されたメッセージ・ブロックの変更された第2半分が、このメッセージ・ブロックの第1半分に代つてUDR200へ記憶され。これと同時に、UDR200に記憶されていた第1半分は、暗号化されたメッセージ・ブロックの第2半分に代つてLDR250へ記憶される。これで、解説プロセスの次の繰返し操作に対する準備ができたことになる。

解説プロセスの2回目の繰返し操作は、サイクル10、11及び12で実行され、サイクル10の間に暗号キー・ビットを1ビット位置だけシフト・ダウンすることによって開始される。暗号キー・ビットのシフト・ダウンは、8ビット幅を介してUKR350及びLKR400の第1段へ印加される

第1信号、SBR線を介して送りの端へ印加される。第1信号、正ひにLDK線を介してすべての端へ印加される信号の前回のもとに行なわれる。SBR及上線の第1信号は、LDK線上の信号と駆動して、UKR350及びLKR400の各々の最終段のピント内容を各々の第1端へ転送させ、一方SBR线上の第1信号は、LDK線上の信号と駆動して、UKR350及びLKR400の各々のピント内容を後続の端へ転送させる。これにより、暗号キー全体の1ピント位置のノット・ダウンが完了され、解説プロセスの2回目の検査し操作のための新しい暗号キー・ピントの組が得られる。この2回目の検査し操作は、暗号化プロセスのところで説明したのと同じようにして、サイクル12で完了される。

前記の様に示されるように、解説プロセスの3回目の検査し操作の開始時には、暗号キーは2ピント位置だけシフトされていなければならぬ。従つて、サイクル11の間に、SBR及上線へ第2信号を印加し且つLDK線へ信号を印加

することによつて、暗号キーの1回目のソフト動作が行なわれ、これにより暗号キーは1ピント位置だけシフト・ダウンされる。暗号キーの2回目のソフトは、サイクル12において、SBR及上線へ第3信号を印加し且つLDK線へ信号を印加することにより行なわれる。同様にして、また所定のソフト計画に従つて、解説プロセスの該段の検査し操作が実行され、サイクル40で最初のプロセスが完了する。ただし、暗号化プロセスのところでも説明したように、16回目の検査し操作では、LB線へ信号が印加されないので、メッセージ・ブロックの第1半分及び第2半分の並置は行なわれない。次のメッセージ・ブロックの解説に対する準備のため、サイクル40の間に、暗号キーの検査シフトが実行され、これにより暗号キーはUKR350及びLKR400内で完全に1回転されて、元の形に戻される。次いで、サイクル40～48の間に、解説されたデータ・メッセージ・ブロックは、UDL200及びモジュロ2加算器650～664の出力からUOB70

0及びLUB750へ各々並列に転送された後、Pボックス800を介して一時に8ピント・バイトずつデータ・バス・アクトの方へ転送される。64ピントの構成されたデータ・メッセージ・ブロックの最後のバイトは、サイクル48で出力され、かくして解説プロセスが完了する。暗号化プロセスの時と同様、図7・及び7・図には示されていないが、解説の暗号化されたデータ・メッセージ・ブロックも同じようにして解説することができる。暗号化プロセスの間にセキュロ2加算器650～664で実行されたセキュロ2加算は、解説プロセスでのセキュロ2加算に上つて逆算されるような自己逆転プロセス(roll-reversing process)であることに注意されたい。

以上説明した本発明の実施例においては、一連のセキュロ2加算器500～514が使用されていたが、積ブロック暗号処理操作は、このようなセキュロ2加算器の使用だけに限定されるものではなく、48ビットの出力をもえるものであれば、任意の他の加算器又はこれらの計算機の組合せ

を使用することができる。更に、本発明に従う暗号装置の構成は、データ・メッセージ・ブロック及び暗号キーのピント数に応じて、容易に変更されるものであり、上述の64ピントの例に限定されるものではない。また本発明に従う暗号装置は、暗号化及び解説の一方のみを実行するだけでなく、両方の動作を並行にするだけで、両方のプロセスを同じ数量で実行し得るものである。

4. 図面の簡単な説明

第1図はデータ处理構成における暗号部屋の設置場所を示すブロック図。第2図は本発明に従う暗号装置の実施例を示すブロック図。第3・乃至第3・図のつながりを明らかにしたブロック図。第3・乃至第3・図は本発明に従う暗号装置の詳細なブロック図。第4図は本発明で使用されるランナ回路の具体例を示す回路図。第5図は第4図のタッチ回路の動作の様子を示すタイミング図。第6図は本発明で使用されるPボックスの詳細を示す回路図。第7・及び7・図のつながりを明らかにしたブロック図。

第7-1及び7-2図は暗号化及び解説プロセスのサイタルを示したタイミング図、第8図は暗号化及び解説プロセスの練習しの様子を示したプロット図である。

500...Pボックス。600...タイミング。100...上部入力バッファ(UTB)。150...下部入力バッファ(LTB)。200...上部データ・レジスタ(UDR)。250...下部データ・レジスタ(LDR)、300...Pボックス。350...上部キー・レジスタ(UKR)。400...下部キー・レジスタ(LKR)。450...Pボックス。500~514...モジュロ2加算器。550~564...8ボックス。600...Pボックス。650~664...モジュロ2加算器。700...上部出力バッファ(UBS)。750...下部出力バッファ(LBS)。800...Pボックス。

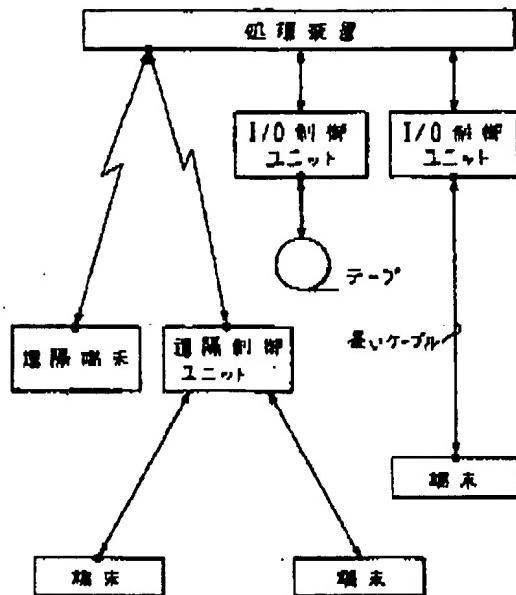
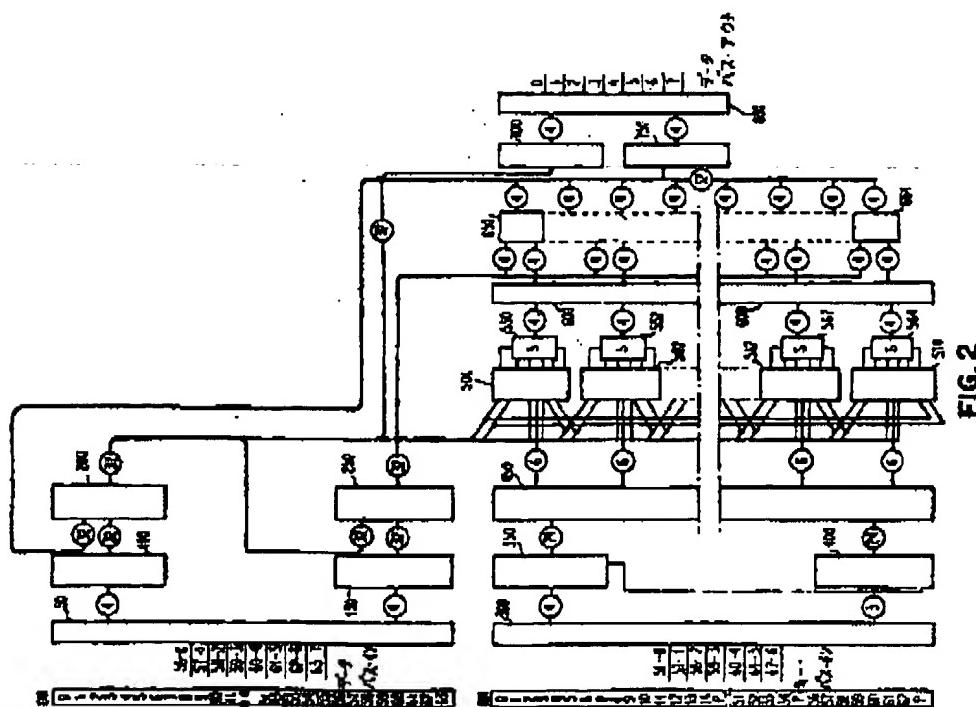
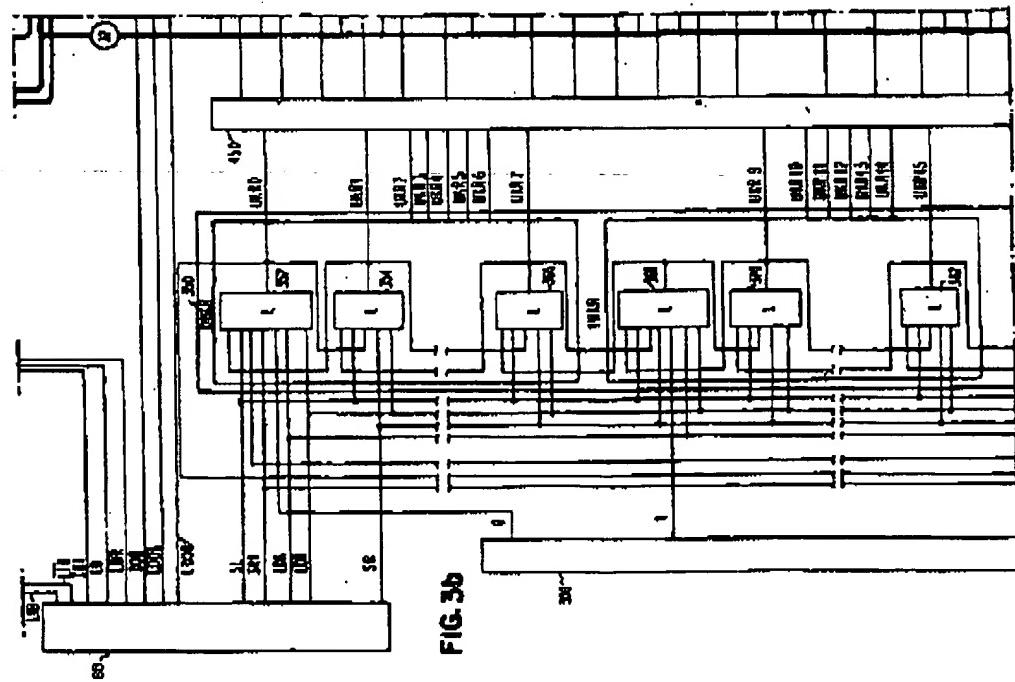
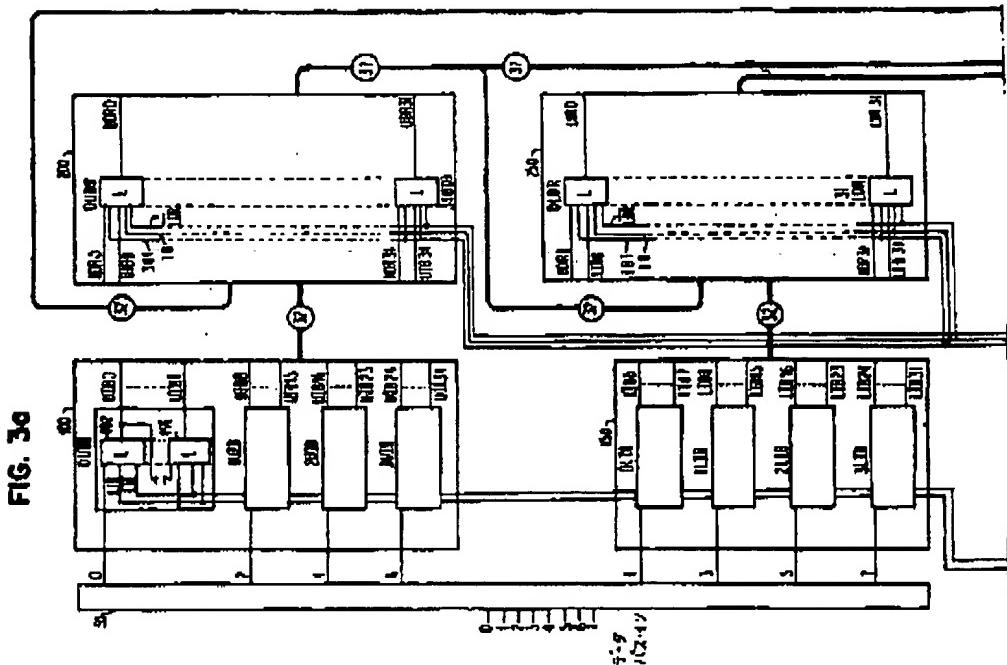
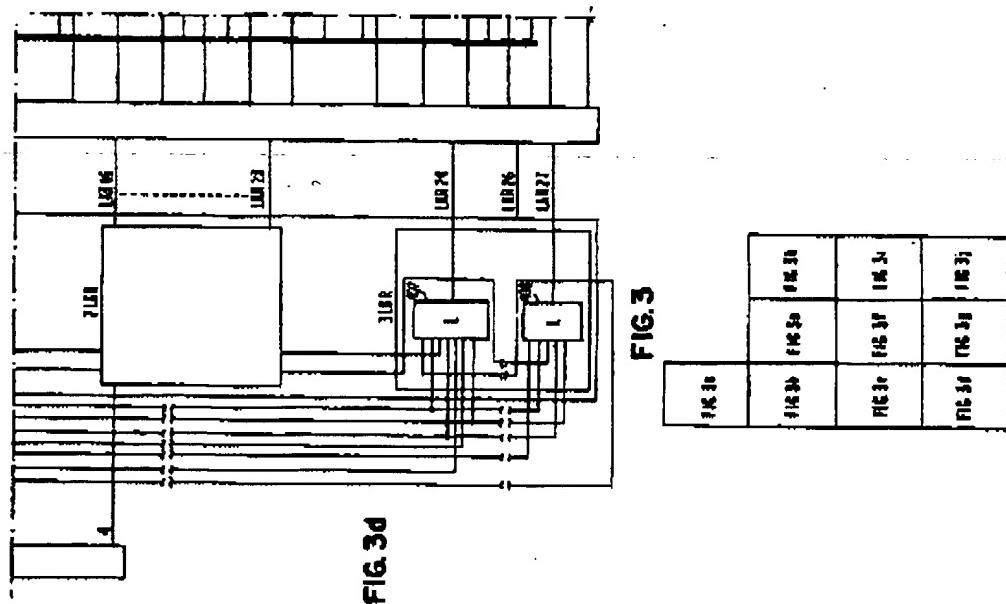
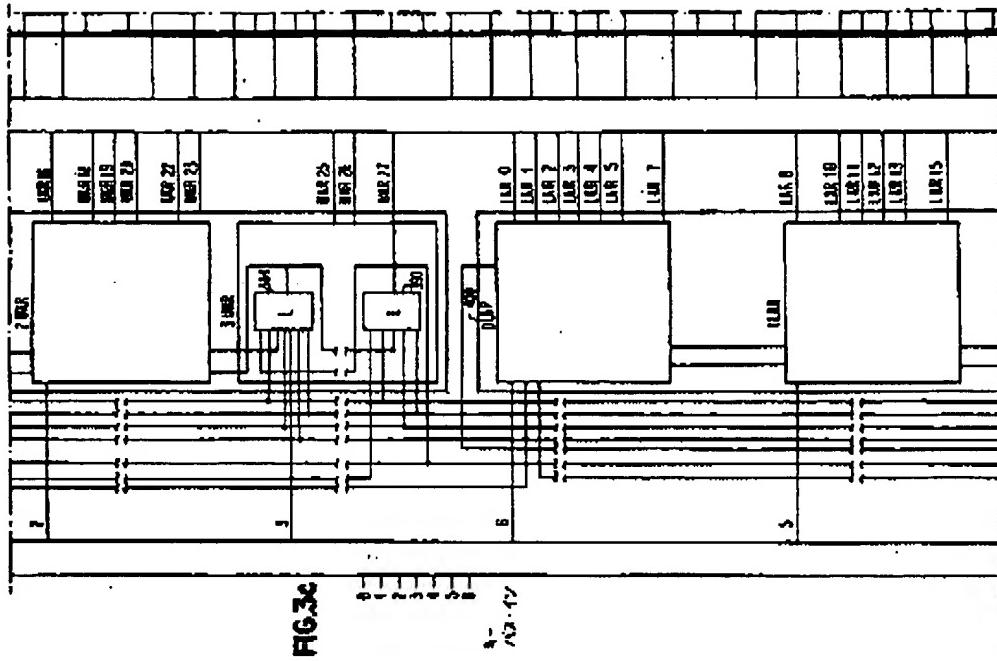


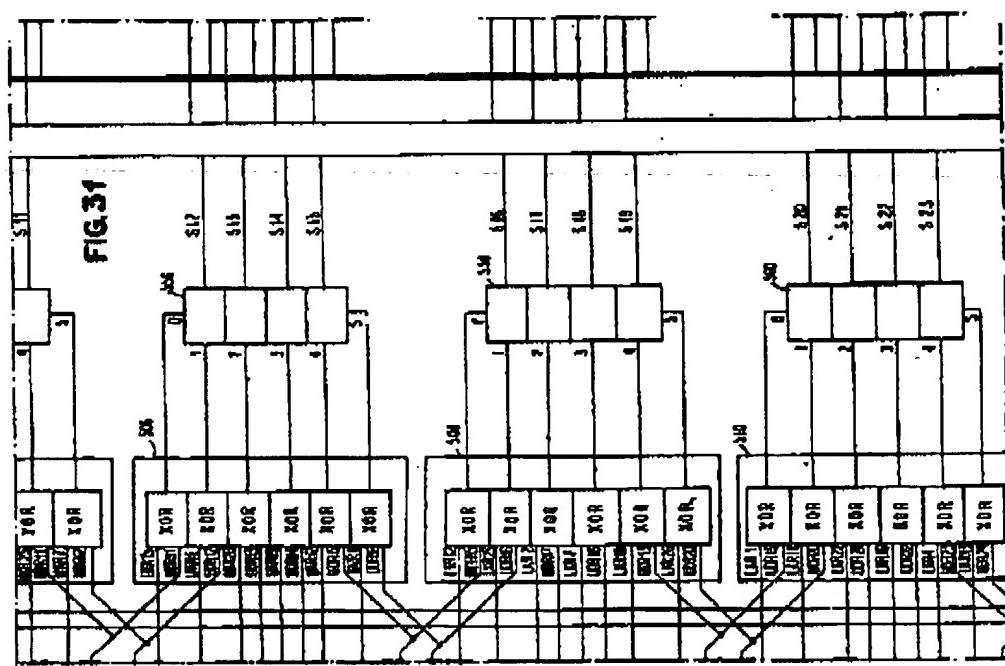
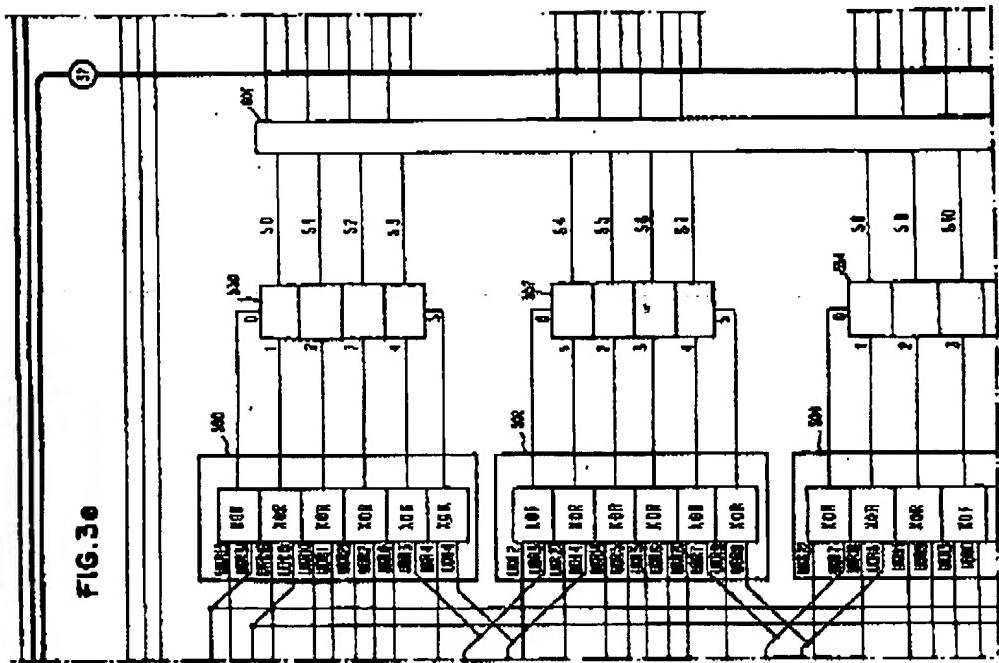
FIG. 1

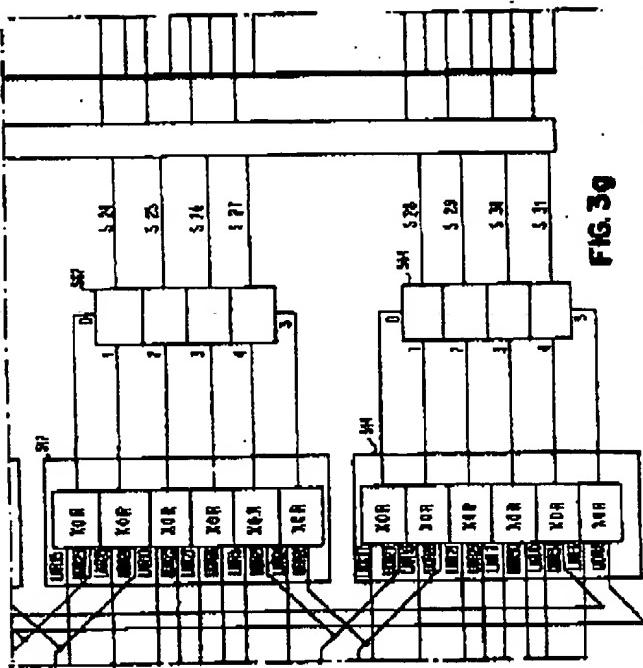


二
五
四

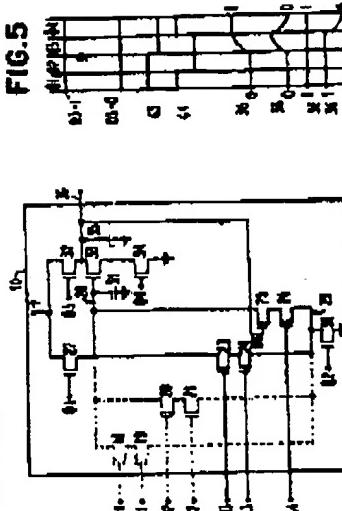








૩૭



四

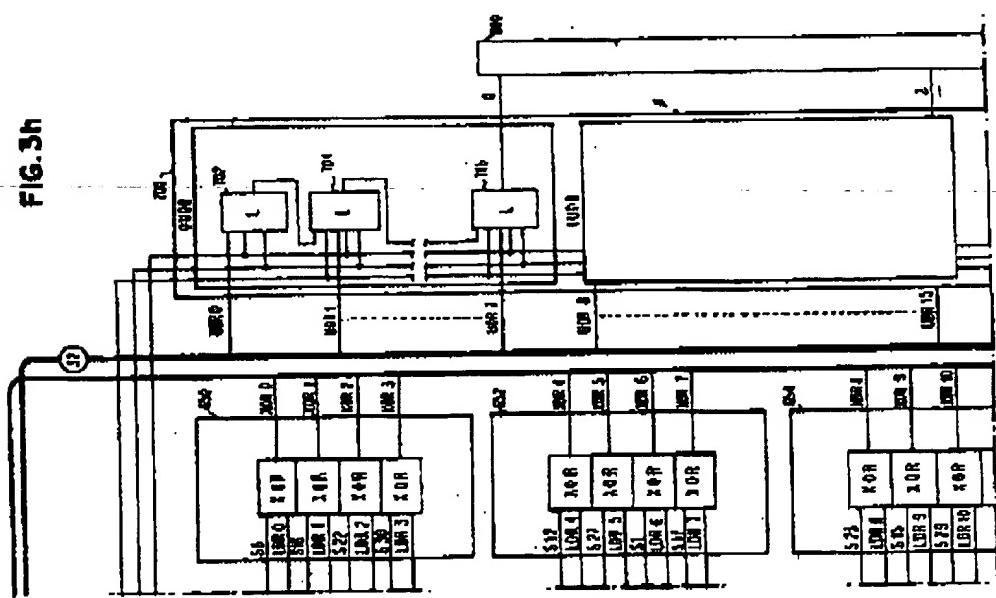


FIG. 3*b*

三

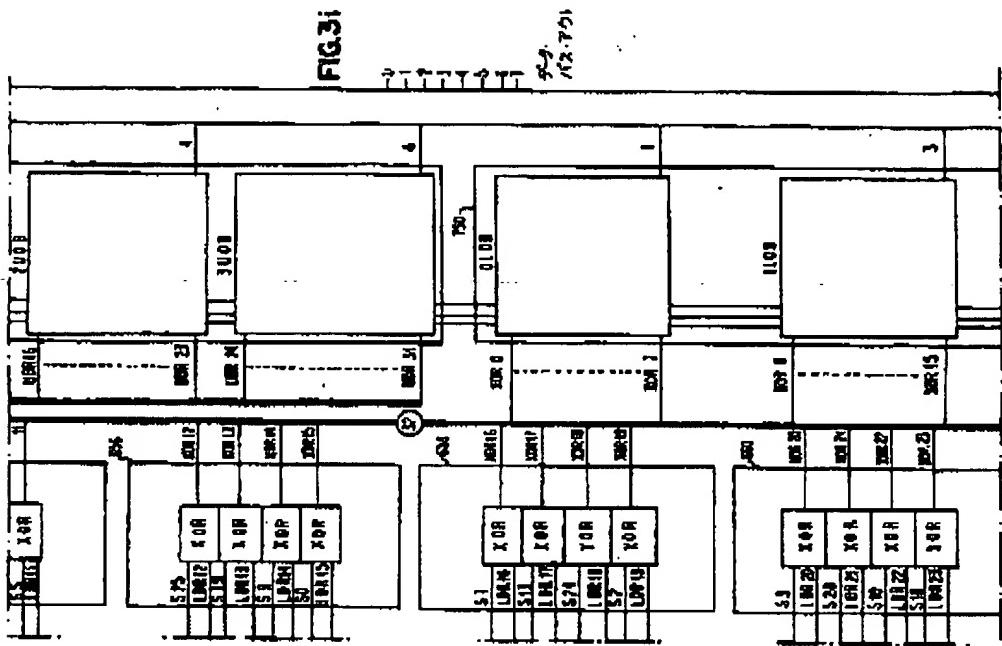


FIG 3

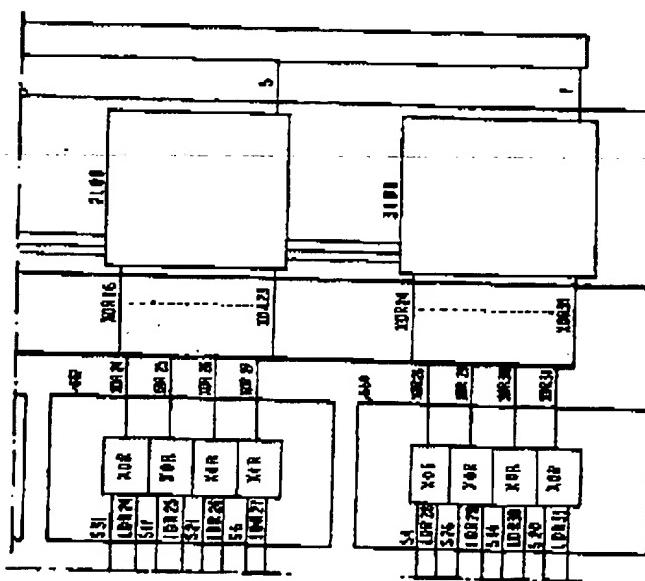


FIG.

FIG. 7a FIG. 7b

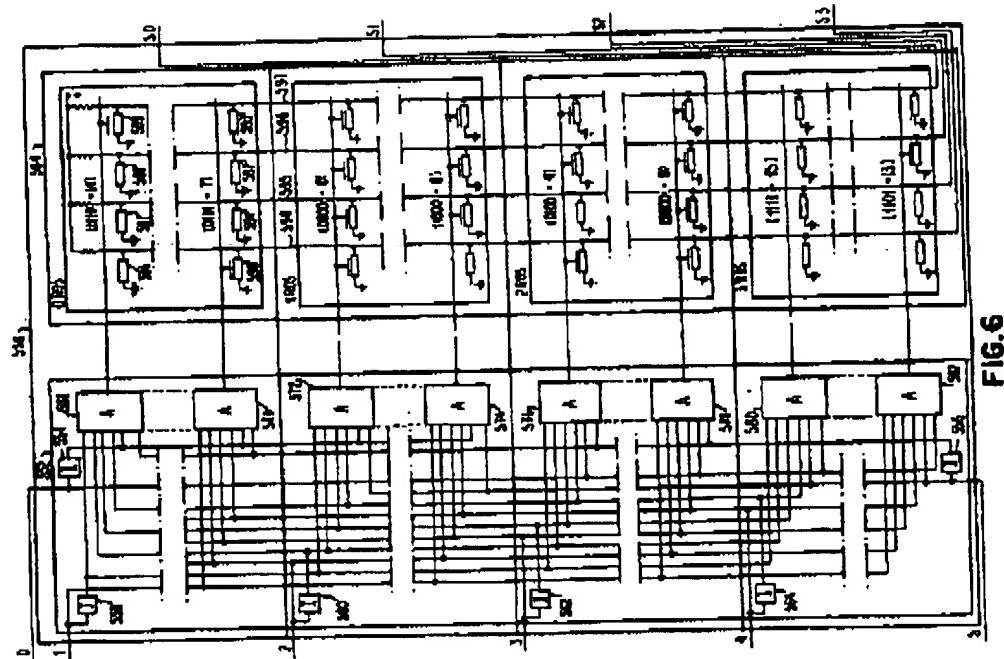


FIG. 6

位相	(25)																										
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
データバス・イン 上の有效バイト	1	2	3	4	5	6	7	8	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
LDR	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
LDR	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
SH	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
データバス・イン 上の初期化バイト	1	2	3	4	5	6	7	8	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
LIB	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
LIB	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
IBT	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
LBR	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
SL (暗号化)	-	-	-	-	-	-	-	-	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
SRR (A4 読)	-	-	-	-	-	-	-	-	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
LB	-	-	-	-	-	-	-	-	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
LDB	-	-	-	-	-	-	-	-	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
DOB	-	-	-	-	-	-	-	-	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
データバス・アウト 上の有效バイト	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

FIG. 7a

FIG. 7b

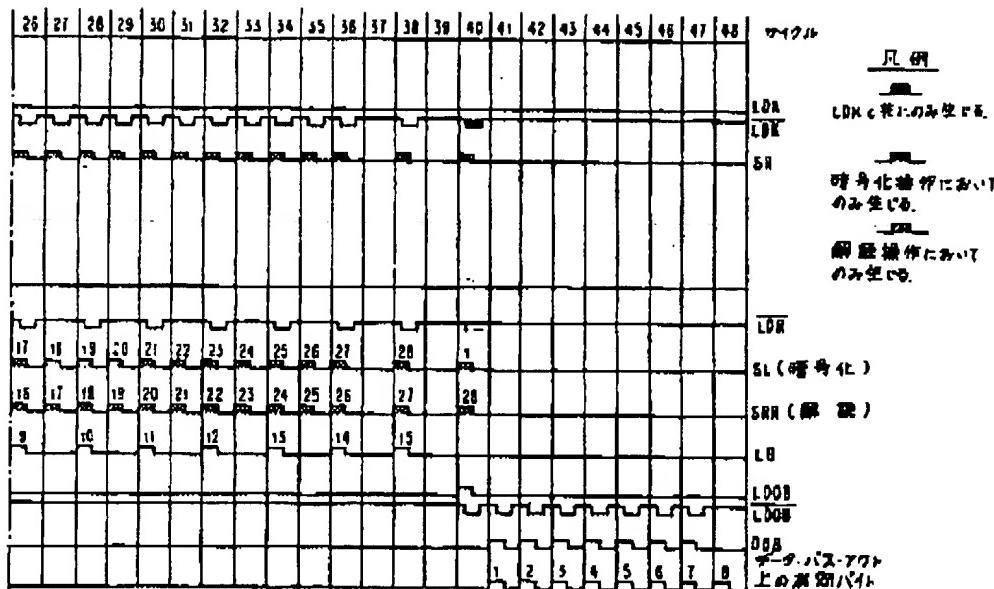
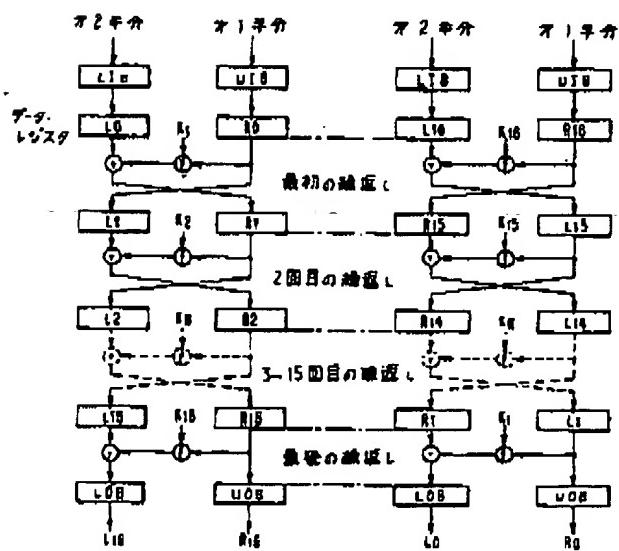


FIG. 8



6. 前記以外の発明者又は代理人

- (1) 発明者
任所 アメリカ合衆国ニューヨーク州インダストン、
ボンクス223-11、アール・ブイ-2、ハート28番地
氏名 ガール・エイケ・ダブリュー・マイヤー
住所 アメリカ合衆国ニューヨーク州ワエスト・ハーレー、
フューリードストーン・ロード12番地
氏名 ロバート・エル・パワーズ
任所 アメリカ合衆国ニューヨーク州ウンドストック、
ホリー・ヒル・ドライブ7番地
氏名 ジョン・エル・スミス
住所 アメリカ合衆国ニューヨーク州ウンドストック、
ホワイトニイ・ドライブ27番地
氏名 ワオルター・エル・タジマ

暗号化

$$\begin{cases} L_0 = R_{k-1}, \\ L_k = L_{k-1} \oplus f(R_{k-1}, S_H), \end{cases} \quad \begin{cases} L_{k+1} = R_k \oplus f(L_k, L_H), \\ R_k = R_{k-1} \oplus f(R_{k-1}, R_H), \end{cases} \quad \begin{cases} L_{k+2} = R_k, \\ R_k = R_{k-1}, \end{cases}$$

解密

$$\begin{cases} L_0 = R_{k-1}, \\ L_k = L_{k-1} \oplus f(R_{k-1}, S_H), \end{cases} \quad \begin{cases} L_{k+1} = R_k \oplus f(L_k, L_H), \\ R_k = R_{k-1} + L_k, \end{cases} \quad \begin{cases} L_{k+2} = R_k, \\ R_k = R_{k-1} - L_k, \end{cases}$$

SUZUYE & SUZUYE

Jpn Pat. Appln. KOKAI Publication No. 51-108701

Filing No.: 51-16096

Filing Date: February 18, 1976

Applicant: International Business Machines Corporation

KOKAI Date: September 27, 1976

Request for Examination: Filed

Int.CI.: H 04 K 1/00

H 04 L 9/00

G 06 F 3/00

Lines 7-16 of Upper Left Column of Page 3

The present invention provides an encrypting apparatus that can perform encrypting processing (encrypting or decrypting) with respect to a 32-bit data block under the control using one arbitrarily-selected encrypting key.

The encrypting apparatus encrypts data by expanding a 32-bit data block into a 48-bit data block. The original data block includes eight segments each having four data bits, and the expanded data block includes eight segments each having six data bits.

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.